JUNE 3, 1987
VOLUME 21, NUMBER 22A

COMPUTERWORLD

FOCUS

Corporate assets in peril

A new vigilance
Thwarting insid
Protecting your
Site uptime man
Special Section:

Computer security

Disaster Recovery Remote Testing Has Been Around for Years...But Never Like This.

Introducing Comdisco Remote Testing

CRT

With the most extensive network of regional Recovery Centers in North America, we've always paid close attention to convenience and cost efficiency on behalf of our customers. With CRT , we're making disaster recovery activity more economical than ever before.

State-of-the-art CRT options extend the reach of our Hot Sites, letting you test your contingency plan from your own office, in any location, at the keyboard of your own 3270 or PC.

The benefits are substantial CRT lets you avoid the cost of travel, meals and lodging for a significant number of your personnel In a test mode, or during an actual disaster, three different CRT options get you into the CDRS Recovery Network—without necessarily having to go there.

We're Comdisco Disaster Recovery Services, Inc. (CDRS)—keeping our customers close through innovation and service.

Yes, CDRS! I'd like to know more. Please contact me regarding the following:

___ CRT (Comdisco Remote Testing)
___ Contingency Planning Services
___ The CDRS Recovery Center in my area
___ Comdisco Data Center Development Services

NAME ____________________ TITLE ____________________

COMPANY ____________________ PHONE ____________________

ADDRESS ____

CITY ____________ STATE ____________ ZIP ____________

Clip and return to Robert E Barrett Manager Marketing Programs CDRS Inc ,
6400 Shafer Court Rosemont IL 60018 Or call 312 698-3000

COMDISCO
Comdisco Disaster Recovery Services, Inc.

Circle Reader Service Number 41

in focus

COVER ILLUSTRATION BY GREG SPALENKA

When other computer companies promise to give you what you need at your desk, they overlook one problem. What you really need is often beyond your desk.

Digital's Networked Desk ties you into your workgroup and into the computing resources and power of your whole organization. So, instead of working alone, you can work together more productively. It starts with a full range of compatible products at the desk—terminals and printers and storage devices, engineering and scientific workstations, personal computers and multi-user super micros. But it goes much further. Within your workgroup, you can

The Networked Desk. Now every member of the team can tie into the computing power of the whole organization.

share the same software and files. You can gain access to all the compute power and resources of the workgroup transparently with our Local Area VAXcluster™ software. Using our new VAXmate™ personal computers, you can run industry-standard PC software on the network. And with our local and wide-area networking capabilities, you can link to anyone, anywhere, on any system.

Digital's Networked Desk. Why work in isolation any more? Call your local Digital sales office. Or write: Digital Equipment Corporation, 200 Baker Ave., West Concord, Massachusetts 01742.

digital™

WITHOUT DATA GENERAL, INTEGRATING YOUR SYSTEMS IS LIKE MIXING OIL AND WATER.

FOR FULLY INTEGRATED BUSINESS AUTOMATION, TALK TO DATA GENERAL.

To maintain a competitive edge, a business needs to integrate all its resources. Ultimately blending people, departments, data and computer systems together.

Data General's Business Automation Systems integrate all these vital elements. Which gives your company one, accessible information flow.

Our industry-leading CEO® software gives you the most integrated business automation essentials. With spreadsheets. Graphics. Decision support. Tools that help you make faster, better informed business decisions.

Then we take you further. By letting you integrate your existing applications.

Our communications story is second to none. We give you the most complete IBM compatibility. We also adhere to industry standards like Ethernet® and X.25.

So our business automation solutions integrate all levels of your company. From PC's to mainframes. And from the next room to the next continent.

Our MV/Family systems lead the industry in price/performance. And give you a low cost of ownership, along with service, training and support.

Today, over 165,000 CEO users have discovered true integrated business automation. To create the best possible blend for your business systems, talk to Data General. Call 1-800-DATAGEN (Canada call 1-800-268-5454.) Or write: Data General, 4400 Computer Drive, MS C-228, Westboro, MA 01580.

Data General
a Generation ahead.

©1987 Data General Corporation. CEO is a registered trademark of Data General Corporation. Ethernet is a registered trademark of Xerox Corporation.

Circle Reader Service Number 43

COMPUTERWORLD
FOCUS

Editorial Director/Editor
Ann Dooley
Managing Editor
Lory Zottola
Features Editor
Michael Tucker
Senior Editor
Stan Kolodziej
Senior Writer
Rebecca Hurst
Assistant Editor
Julie Cook
Editorial Assistant
Catherine Gagnon

Display Advertising Manager
Maureen Carter
Production Director
Peter Holm
Senior Production Manager
Leigh Swearingen
Art Director
Tom Monahan
Design Consultant
Ronn Campisi
Typesetting Manager
Carol Polack
Production Assistants
Christopher P Cuoco, Beverly Wolff

Computerworld Editor in Chief
Bill Laberis

Board Chairman
Patrick J McGovern
Chief Executive Officer
CWCI, Inc.
Axel Leblois
Publisher/President
CWCI-Framingham
Lee Vidmer
Vice President/Research
Jack Edmonston
Vice President/Sales
Edward P Marecki

Computerworld Focus is a publication of IDG Communications the world s largest publisher of computer-related information. IDG Communications publishes over 80 computer publications in more than 28 major countries. Fourteen million people read one or more IDG Communications publications each month. IDG Communications publications contribute to the IDG News Service offering the latest on domestic and international computer news. IDG Communications publications include ARGENTINA'S *Computerworld Argentina PC Mundo,* ASIA'S *Communications World Computerworld Hong Kong, Computerworld Indonesia Computerworld Malaysia, Computerworld Singapore, Computerworld Southeast Asia PC Review* AUSTRALIA'S *Computerworld Australia Communications World Australian PC World, Australian Macworld,* AUSTRIA'S *Computerwelt Oesterreich,* BRAZIL'S *DataNews, PC Mundo Micro Mundo,* CHILE'S *Informatica Computacion Personal,* DENMARK'S *Computerworld Danmark PC World Danmark,* FINLAND'S *Mikro, Tietoviikko,* FRANCE'S *Le Monde Informatique Distributique InfoPC, Le Monde Des Telecoms* GREECE'S *Micro and Computer Age* HUNGARY'S *Computerworld SZT Mikrovilag* INDIA'S *Dataquest,* ISRAEL'S *People & Computers Weekly People & Computers Biweekly,* ITALY'S *Computerworld Italia,* JAPAN'S *Computerworld Japan,* MEXICO'S *Computerworld Mexico,* THE NETHERLANDS *Computerworld Netherlands, PC World Benelux,* NEW ZEALAND'S *Computerworld New Zealand,* NORWAY'S *Computerworld Norge PC World Norge* PEOPLE'S REPUBLIC OF CHINA'S *China Computerworld, China Computerworld Monthly* SAUDI ARABIA'S *Arabian Computer News* SOUTH KOREA'S *Computerworld Korea PC World Korea,* SPAIN'S *Computerworld Espana, Commodore World, PC World Espana Communicaciones World Informatica Industria,* SWEDEN'S *ComputerSweden Mikrodatorn, Svenska PC World,* SWITZERLAND'S *Computerworld Schweiz,* UNITED KINGDOM'S *Computer News, DEC Today, ICL Today PC Business World,* UNITED STATE'S *Amiga World, Boston Computer News, CD-ROM Review Computerworld Computers In Science, Digital News, Federal Computer Week 80 Micro FOCUS Publications, InCider Infoworld, Macworld Computer + Software News (Micro Marketworld/Lebhar Friedman) Network World PC World, Portable Computer Review Publish! PC Resource Run,* VENEZUELA'S *Computerworld Venezuela,* WEST GERMANY'S *Computerwoche PC Welt, Run Information Management, PC Woche*

Write Us

We welcome letters to the editor and publish those we judge to be of interest to our readers. Letters should be addressed to the Editor.
Computerworld Focus, 375
Cochituate Rd., Box 9171
Framingham, MA 01701-9171

FROM THE EDITOR

Better safe than sorry

A breach in your organization's computer security is an accident waiting to happen. Although the realization of the need for security is growing, not enough action is taking place. In the story on page 23 detailing a recent Ernst & Whinney survey, 87% of the respondents recognized the increasing importance of security issues, but only 6% felt their companies were adequately protected. And a *Focus* survey of MIS managers on page 21 showed similar results.

Good intentions are obviously not enough. It is easy to underestimate how integral computers and the information they hold have become to businesses. Figures show that the cost of interrupted DP services due to water damage for a large insurance company would be $275,000 per day; interrupted services for a major airline could cost it $20,000 per minute! Disaster recovery, this month's Special Section topic, has become a big market.

And threats to security do not always come from without. Hackers may get the headlines, but the majority of data theft is perpetrated by insiders. Computer security has become a people problem because the best security devices and procedures in the world won't protect against carelessness by management and employees. Businesses, unsure of legal protections, don't want to admit to the public or their competitors that they are vulnerable to tampering and usually keep news of computer crimes under wraps. It will take a massive education effort — spearheaded largely by MIS — to goad management and employees into turning this situation around.

However, as MIS emphasizes the importance of data security practices, it shouldn't make the systems too difficult to use. MIS should weigh the issues and make trade-offs between security protection and end-user computing. For example, Has the system become so secure and unapproachable that people are bypassing it? Does every company or department need the same set of stringent safety requirements? Has the cost exceeded the value of the information involved? The need for protection has never been greater, and it's up to MIS to achieve a secure yet effective system.

Ann Dooley

Big Blue will sell no product before its time

I was startled at Amy Wohl's contention [*CW Focus*, March 4] that IBM is "too big and too structured to be very flexible; whatever it has decided to do . . . was decided a long time ago."

The company uses its enormous resources to develop hardware and software products in parallel, and the Golden Boys (as I call the members of its management committee) only need to choose among the alternatives at the last moment.

IBM can afford to put the plans for a product on the shelf until those Golden Boys decide the time is ripe.

An example of the parallel strategy is the advent of the 360 in 1964, when alternatives like the 7095 were kept alive until a few days before the unveiling.

An example of the shelving strategy is the Selectric typewriter, which was held for many months until the time was judged right to announce it.

[redacted]

Herbert R J. Grosch
Association for Computing Machinery
Mies, Switzerland

A closer link sought between the classroom and workplace

In a letter in the January issue of *Computerworld Focus*, a computer science student complained that his education lacked hands-on training and left him ill prepared to find employment. The student rightly asks what we, as educators, can do about this type of situation.

- Solicit advice from industry experts when designing curricula
- Recruit and promote faculty members who have significant data processing experience.
- Ensure that laboratories in which students acquire hands-on skills are equipped with up-to-date hardware and software systems.

Effective preparation for the real world depends on establishing a close link between the classroom and the workplace

Philip A Clement
President
Devry Institute of Technology
Evanston, Ill

IBM's secret weapon to shake crowded System/36 market?

I recently read "Is IBM In The PC Business?" [*CW Focus*, March 4] and have a few comments:

- IBM made a strategic blunder when it opted for third-party components to make the Personal Computer. This move got the PCs to market quickly, but the long-term effects have been to show customers that a computer can function effectively without those three little letters.
- We see plug-compatible machines at both the low and high ends of the computer spectrum, and shortly many manufacturers will attack the System/36 market

IBM can and will improve its market position with increased PC functions, but to return to the profitable days of yesteryear, it must leverage proprietary hardware and software. I predict that one of IBM's next moves will be to enhance the PC with a version of IBM's System/36 multiuser operating system — SSP — giving it RPG-II capabilities, retaining DOS and providing a simple and logical growth path for the user.

Vince Cannuscio
Vice-President
Notional Computer Solutions, Inc
Huntington Station, N Y

Q AND A

Connie Brock

Once burned, twice shy: A disaster survivor offers advice on how to safeguard your DP operations.

Connie Brock is the vice-president and data security officer for Norwest Technical Services, Inc., a subsidiary of Norwest Corp., both of Minneapolis. Brock, who has been with Norwest since 1969, has been responsible for the company's disaster recovery plans during the past four years.

On Thanksgiving Day 1982, a major fire broke out in the company's Northwestern National Bank headquarters. However, because of the company's extensive disaster recovery plan, the fire did not affect DP operations. Since then, the firm has been active in promoting disaster recovery planning to businesses both in and outside the banking industry. Brock spoke recently with *Computerworld Focus* Senior Editor Stan Kolodziej

Did the Northwestern bank fire create increased concern about disaster recovery planning?

Yes. The bank fire was terrific for increasing the awareness about the possibility of disaster and what it could mean to businesses. I think what really started [the interest] rolling, however, was a big study released by the University of Minnesota before that, about 10 years ago. The study looked at businesses that had suffered disasters and looked at their survival rates.

It concluded that most businesses really had to recover critical operations within 30 hours. If they couldn't do that, then the likelihood of long-term business survival was very low. That study formed the base on which a lot of companies built their disaster recovery plans.

Is there enough awareness now about the importance of disaster recovery?

There's much more awareness than there was five years ago, but I don't think it's adequate yet. The trick is for companies to correctly identify which of their business operations are the critical ones that they need to recover and survive. Beyond that, they have to establish what their minimum acceptable level of operation is and the maximum time frame required to achieve that minimum level.

Companies should stay focused on those questions and not be distracted about whether it's cost-effective to have total recovery capability. Forget cost concerns. The important point is first knowing how you will survive as a business.

What, in your opinion, is the single most important issue in disaster recovery planning?

Maintaining the plan. If you hire people to come in and form a plan for you, what happens when they're gone? Companies should maintain their own disaster recovery plans. Part of the maintenance is realizing that your business is going to change. Periodically, you have to go into the plan and ask if the right critical operations are still defined, if there are correctly defined minimum levels of operation and if recovery time frames are still workable. The basic thrust is to see if the plan is still current and still works.

I think a lot of organizations start out with a pretty good disaster recovery plan but let it fall by the wayside because they don't put the resources into an ongoing maintenance program. If you do it yourself, you build expertise and awareness, and it's easier to establish an ongoing maintenance mode.

How important is it to get end users involved in the actual testing?

Always important. We'll frequently have users available as part of the test. During a test, users will be at their normal business locations conducting business as usual. When we send a team to our hot site location during a test, we are also testing users in the field at the other end. It very much simulates the real world.

How often do you test your plan?

At least twice a year. We go through some very careful planning before the test to make sure that we're clear on what the test objectives are. We'll place a special emphasis on anything that might have changed since the last test. If we've added a new product or service, for example, it will get special attention on the next test.

Continued on page 9

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST CLASS PERMIT NO 124 DALTON MA 01227

POSTAGE WILL BE PAID BY ADDRESSEE

Computerworld Focus
Post Office Box 300
Dalton, MA 01227-9882

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST CLASS PERMIT NO 124 DALTON MA 01227

POSTAGE WILL BE PAID BY ADDRESSEE

Computerworld Focus
Post Office Box 300
Dalton, MA 01227-9882

COMPUTERWORLD FOCUS

Reader Service Card
Issue: June 3/Expires: August 5, 1987

Please Use This Card For Product Information

Name______________ Title ______________
Company ______________ Phone ______________
Address ____________________________
City______________ State_______ Zip _______

A Please check the business industry in which you work (check one)

End Users
1 □ Manufacturer (other than computer)
2 □ Finance/Insurance/Real Estate
3 □ Medicine Law/Education
4 □ Wholesale/Retail Trade
5 □ Business Service (except DP)
6 □ Government - State/Federal Local
7 □ Public Utility/Communication Systems/Transportation
8 □ Mining/Construction Petroleum Refining
9 □ Other User ________ (please specify)

Vendors
10 □ Manufacturer of Computers Computer Related Systems or Peripherals
11 □ Computer Service Bureau Software/Planning/Consulting
12 □ Computer/Peripheral Deeler Distributor Retailer
13 □ Other Vendor ________ (please specify)

B Pleese check your mein job function (check one)
1 □ Corporate Management
2 □ Financial Management
3 □ MIS DP Management
4 □ MIS DP Operations
5 □ Data Communications Management
6 □ Data Communications Operations

C Reeson for this inquiry (check one)
1 □ Immediate purchase
2 □ Future purchase
3 □ Information only

D Is this your personel copy of Computerworld Focus? (check one)
1 □ My personal copy
2 □ I'm a pass along reader

E Pleese check the number of employees in your company (check one)
1 □ Over 1 000 employees
2 □ 501 1 000 employees
3 □ 500 or under

Circle the # that corresponds to the number at the bottom of the item in which you are interested

1	21	41	61	81	101	121	141	161	181
2	22	42	62	82	102	122	142	162	182
3	23	43	63	83	103	123	143	163	183
4	24	44	64	84	104	124	144	164	184
5	25	45	65	85	105	125	145	165	185
6	26	46	66	86	106	126	146	166	186
7	27	47	67	87	107	127	147	167	187
8	28	48	68	88	108	128	148	168	188
9	29	49	69	89	109	129	149	169	189
10	30	50	70	90	110	130	150	170	190
11	31	51	71	91	111	131	151	171	191
12	32	52	72	92	112	132	152	172	192
13	33	53	73	93	113	133	153	173	193
14	34	54	74	94	114	134	154	174	194
15	35	55	75	95	115	135	155	175	195
16	36	56	76	96	116	136	156	176	196
17	37	57	77	97	117	137	157	177	197
18	38	58	78	98	118	138	158	178	198
19	39	59	79	99	119	139	159	179	199
20	40	60	80	100	120	140	160	180	**200**

□ I have circled #200 on the Reader Service Card to enter my *Computerworld* subscription for one year 51 weekly issues and 12 *Computerworld Focus* issues for $44 and please bill me later This rate valid only in the U S

①

COMPUTERWORLD FOCUS

Reader Service Card
Issue: June 3/Expires: August 5, 1987

Please Use This Card For Product Information

Name______________ Title ______________
Company ______________ Phone ______________
Address ____________________________
City______________ State_______ Zip _______

A Pleese check the business industry in which you work (check one)

End Users
1 □ Manufacturer (other than computer)
2 □ Finance/Insurance/Real Estate
3 □ Medicine/Law/Education
4 □ Wholesale/Retail/Trade
5 □ Business Service (except DP)
6 □ Government - State/Federal Local
7 □ Public Utility/Communication Systems/Transportation
8 □ Mining/Construction/Petroleum Refining
9 □ Other User ________ (please specify)

Vendors
10 □ Manufacturer of Computers Computer-Related Systems or Peripherals
11 □ Computer Service Bureau/ Software/Planning/Consulting
12 □ Computer/Peripheral Dealer Distributor/Retailer
13 □ Other Vendor ________ (please specify)

B Pleeee check your mein job function (check one)
1 □ Corporate Management
2 □ Financial Management
3 □ MIS/DP Management
4 □ MIS/DP Operations
5 □ Data Communications Management
6 □ Data Communications Operations

C Reeson for this inquiry (check one)
1 □ Immediate purchase
2 □ Future purchase
3 □ Information only

D Is this your personel copy of Computerworld Focus? (check one)
1 □ My personal copy
2 □ I'm a pass along reader

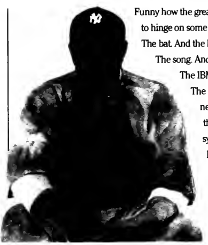
E Pleese check the number of employees in your compeny (check one)
1 □ Over 1 000 employees
2 □ 501 1 000 employees
3 □ 500 or under

Circle the # that corresponds to the number at the bottom of the item in which you are interested

1	21	41	61	81	101	121	141	161	181
2	22	42	62	82	102	122	142	162	182
3	23	43	63	83	103	123	143	163	183
4	24	44	64	84	104	124	144	164	184
5	25	45	65	85	105	125	145	165	185
6	26	46	66	86	106	126	146	166	186
7	27	47	67	87	107	127	147	167	187
8	28	48	68	88	108	128	148	168	188
9	29	49	69	89	109	129	149	169	189
10	30	50	70	90	110	130	150	170	190
11	31	51	71	91	111	131	151	171	191
12	32	52	72	92	112	132	152	172	192
13	33	53	73	93	113	133	153	173	193
14	34	54	74	94	114	134	154	174	194
15	35	55	75	95	115	135	155	175	195
16	36	56	76	96	116	136	156	176	196
17	37	57	77	97	117	137	157	177	197
18	38	58	78	98	118	138	158	178	198
19	39	59	79	99	119	139	159	179	199
20	40	60	80	100	120	140	160	180	**200**

□ I have circled #200 on the Reader Service Card to enter my *Computerworld* subscription for one year 51 weekly issues and 12 *Computerworld Focus* issues for $44 and please bill me later This rate valid only in the U S

②



Funny how the greatest success stories always seem to hinge on some special combination.

The bat. And the hitter.

The song. And the singer.

The IBM 9370. And VMCENTER II.

The 9370's potential for greatness has never been in doubt. But it takes more than potential to make departmental systems run smoothly throughout large organizations.

What it takes—is VMCENTER II.

THE ACCESS USERS NEED. THE CONTROL YOU NEED.

VM CENTER II AND THE 9370: A HARD-HITTING COMBINATION.

VMCENTER II is VM Software's newest, most comprehensive answer to the systems management needs of the VM operating environment—the environment best suited to the overwhelming majority of 9370 users.

In one easy-to-use package, VMCENTER II brings computing power to the people who need it at every organizational level. Equally important, VMCENTER II helps maintain strong central control while vastly reducing the tasks traditionally faced by data processing professionals in interactive user environments.

System security. DASD management. Performance monitoring. Project accounting. They may sound mundane. But they're critical to smooth-running applications. And VMCENTER II takes care of them all—plus a lot more.

All this while users are enjoying dependable, easy access to a system that performs at its peak, day after day. And even helps them plan ahead for future needs.

THE POWER. AND THE GLORY.

The 9370 marks a great opportunity for your entire organization. But to make the most of it, there's nothing like VMCENTER II.

After all, VMCENTER II is based on the original VMCENTER—the world's leading VM data center management system. And it's loaded with new features specifically designed for departmental environments.

The result is a system that's a potent partner for the 9370. A sure way to simplify a major transition for your organization. And an all-round clutch performer that'll make *you* look good for choosing it.

VMCENTER II. For more information call **1-800-562-7100**

(In Virginia or outside the Continental U.S. 703-264-8000). Or write VM Software, Inc., 1800 Alexander Bell Drive, Reston, Virginia 22091.

Babe Ruth's bat courtesy of The Major League Baseball Players Alumni Association
© 1987 VM Software, Inc.

CWX 870603

VM SOFTWARE INC.

Circle Reader Service Number 46

VMCENTER II FROM VM SOFTWARE, INC.

COMMENTARY

Think like a criminal

Sanford Sherizen

If you think that crime doesn't pay, you haven't met a computer criminal. Not only can crime pay quite a bit, but increasingly, it is perpetrated by authorized employees.

An excellent way for senior-level executives to protect their organizations from such offenses is to learn how to think like a thief.

The following are some of the ways by which computer criminals, particularly employees who are given access to equipment as part of their work, are committing crimes. These rules will show how criminals think and what companies should look for to prevent these acts.

- **Work the odds.** As a criminal, understand that while many organizations are required to prevent computer crime, few can recognize it or know how to detect it, how to investigate it or what to do if it happens to them. A computer criminal's best protection is that the majority of these crimes are found out by chance and that, even if found, most organizations are not willing to press charges. The odds of being able to perform a crime and get away with it are in your favor.

- **Know the limits of the law.** Find out if your state has a computer crime law and wbether anyone has ever been prosecuted under it. Go where the law is the weakest or where public prosecutors are least interested in handling computer crime cases.

- **Learn how other criminala avoid detection.** To commit a computer crime, you need to know how a particular organization processes its work, what the control weaknesses that allow crimes to occur are and how you can get away with a crime. Your weakest area is probably knowing how to cover your tracks and not leave fingerprints. Remember, do not commit too many crimes; steal small amounts over a long period of time. Continue with your usual lifestyle, and do not buy big, expensive cars or take trips around the world — yet. Choose your confederates in crime carefully. Learn how to be a loyal employee that nobody would suspect.

- **Pick your opportunities.** You have the advantage as an employee to choose the best time and way to hit a system. Vacation and slack times like tbe month of December and Friday afternoons are convenient. At these times, employees are under pressure to complete jobs or close the books and little attention will be paid to work as long as it looks almost right.

Also, borrow passwords from co-workers if you can; or better yet, try to get one password for everyone in your office then post it for all to use. That way it becomes difficult to pin any computer discrepancies on you specifically

- **Become known as a computer hater.** Most bosses expect computer criminals to be high-tech nerds. Complain about computers and get a reputation as one of the most technophobic people in the office. Refuse to have even a bank automated teller machine card, and then quietly learn all you can about computer applications and get hold of books on computer crimes, hacking and security.

- **Learn how computers undercut controls.** Find out which management controls have been weakened by computerization. Like those who investigate crimes, follow money trails and see if there are opportunities for crime. See what the lack of source documents may mean to you, and discover how electronic mail may provide you with information.

- **Test a firm's defenses by making mistakes.** Find out if there is anyone behind the terminal that is electronically watching what you do. One way to discover if there is surveillance is to make mistakes and see what happens. Do not make the same error continually but rather try things periodically that might allow you to change data for your own advantage. If someone contacts you to ask what you are doing, become technophobic and blame the computer. If no one contacts you about your mistakes, continue your testing long enough to gather information. Then stop for a while and prepare yourself for the big hit.

- **Try to work for a boss who ia afraid of computers.** If you happen to have a boss who dislikes technology, you are in luck. If you are stuck with a power user, transfer to a department in which, as long as the system seems to be running, the boss doesn't bother anyone or check their work.

- **Copy information rather than steal money.** Understand that information is worth more than traditional forms

Sherizen is a Natick, Mass -based information security consultant and criminologist

VIEWPOINT

of property. In other words, steal the data in the computer rather than the computer. Not only is information lighter, but it will also provide you with a bigger monetary payoff. Consider what your company's competitors are interested in, think about how the information you handle can be used for your own purposes and become more aware of the intangible properties that make today's businesses run.

• **Check how open the company is to countersuits.** Consider what the grounds are for protecting yourself in the event of detection.

Take into account whether you have seen a written copy of the company's computer crime policy or if you have had to sign a statement saying you have been briefed on these procedures.

Are there what the law might consider adequate attempts to protect company assets and resources? Finally, find out if there are sufficient audit trails that establish you, and you alone, as the perpetrator of the crime. If there are no such safeguards, congratulations! You may be free to perform all sorts of criminal acts without fear of punishment.

• **Be willing to be fired**. The chances of being detected are minimal, but sometimes mistakes happen. If you are caught, act penitent, horrified that you could have done such a thing and feign a nervous breakdown. Chances are that management will let you go quietly to save everyone from further embarrassment. Take the money and run.

If the company insists upon the money's return, try to negotiate. Negotiations should include the following prospects: volunteer as an internal consultant to help prevent computer crime from happening again; return part of the money and ask the company to drop the charges or you will publicly embarrass it; or tell the firm you need a glowing letter of recommendation so that you can get another job to pay back the money.

By knowing these rules, you will be able to think as a successful computer criminal does and protect yourself. By using these rules, you won't have to worry about what to do after retirement — consider movie rights.

Q&A

Continued from page 6

Computers seem to have become the pivotal point in corporate disaster recovery planning. Would you agree?

Yes, that's happened during the past five years. Businesses have begun to recognize their growing dependence on information systems. But it doesn't mean that disaster recovery is completely a DP issue; that's a misconception. What may have looked like a DP issue 10 years ago looks more like a business survival issue now, just because of the growth in automation and the growing dependency on information services in all businesses — not just banking and financial services.

A lot of times, information systems are the focal point for disaster recovery planning, and usually, when you start with MIS, you wind up covering most of the critical business functions whether or not they're automated. That's a good entry point.

Is there a chance that disaster recovery planning is being oversold by consultants and the rest of the industry?

The marketing can tend to lean too mucb toward scare tactics and, in that way, can actually be counterproductive. If you overplsy any issue, people will not pay attention to it. I also think that although there are many companies selling consultation services and actually writing up plans, these firms don't have the obvious credibility with senior management that those people who experienced disasters firsthand have. That's why for years after we had our fire, we had many requests for people to come and talk [to us] about nur experience. The fact that we weren't selling anything didn't hurt.

Do you think most large companies have the internal resources to handle their own disaster recovery planning? Do you think they might be relying too much on consultants?

I think the most effective approach is to handle disaster recovery planning with your own people. It's worked well for us. We have one full-time specialist in our organization who handles disaster recovery planning. At her disposal is a contingency coordinator team made up of managers from each of the line units. This team has the responsibility for our entire contingency preparedness program.

When you [create a plan] internally, you get much greater awareness throughout the company about the issues associated with disaster recovery planning. You have an educated base, and you have the line people participating and making decisions about what's necessary to ensure business survival. You don't have to pay a lot of money for a consultant [if you write the plan yourself]. It's cheaper to do it this way. I would even argue that you get a better result. Even the cost of keeping a full-time recovery person is [minimal] when business survival is at stake.

What's the one message you'd give to those expanding their disaster recovery plans?

Remember that even though the probability of a disaster is very low, the impact is very severe.

ONCE AGAIN, STRATUS CATCHES THE COMPETITION WITH THEIR COMPUTERS DOWN.

It never fails. Every few years Stratus comes out with a new generation of fault-tolerant computers whose price/performance and reliability are a source of astonishment to our market and a source of embarrassment to our competitors.

This year is no exception. With the introduction of our new XA2000 family, Stratus now offers the best performing, most powerful fault-tolerant computer systems in the world. Systems powerful enough to handle the largest on-line transaction processing applications with the lowest cost per transaction in the industry. Systems with more computing power than ever before, enhancing the performance of what was already the world's most reliable architecture – hardware-based fault tolerance.

Our new Model 140, for example, can execute over 50 transactions per second. That's more than three times the processing power of a Stratus XA600 – which up till now was the most powerful hardware-based fault-tolerant system you could buy. And if you *did* buy one, don't worry: all Stratus computer systems, old and new, are completely compatible.

Stratus XA2000 performance becomes even more impressive when you begin adding systems. In fact, you can interconnect thousands of Stratus computers into local and wide area networks for virtually unlimited performance.

INTRODUCING THE STRATUS XA2000 FAMILY.

THE WORLD'S MOST RELIABLE COMPUTER JUST GOT THREE TIMES MORE POWERFUL.

Upgrading couldn't be easier. Or faster. Because all you do is add boards. You can even do it while the system is running.

And the unique, "open-ended" architecture of our new XA2000 gives you the flexibility to begin building your foundation now for the more sophisticated applications you'll be running years from now.

Our XA2000 family includes four totally compatible, instantly upgradable computer systems: the Models 110, 120, 130, and 140. Each more powerful than the one before it. And each years ahead of its time in speed, upgradability, reliability, and above all, price/performance.

All this from a company that enjoys the highest level of customer loyalty in the industry: a recent *independent* survey of some of our customers revealed that 100% of those surveyed would not even consider changing computer companies.

So, for complete information, contact your local Stratus sales office, or call Peter Kastner at (617) 460-2192.

Because you may not see another computer like this until the 21st century.

Stratus®
CONTINUOUS PROCESSING™

Stratus Computer, 55 Fairbanks Boulevard, Marlboro, MA 01752

Circle Reader Service Number 48

MANAGER'S CORNER

A measure of desktop success

Jim Young

In the life of every investment, every trial, every pilot program, there comes a moment of truth. Such a moment is rapidly approaching for end-user computing.

The end-user computing industry is approaching the point at which management is waiting to learn how fundamentally valuable this computing concept has proven to be. It would be nice if executives and MIS could look at user budgets, key measurements of output or other quantitive criteria to see if a company is better off. But other factors cloud this comparison, and, more importantly, such an analysis would ignore some of the qualitative benefits that technologists have told organizations to expect. To measure intangible benefits, we must resort to the techniques of observation and judgment.

We must first ensure that our more skeptical colleagues were not correct in predicting that end-user computing would have detrimental effects. There should be no stand-alone use of the technology when centralized techniques are required. There should be no data pollution introducing errors and inaccuracy to valid facts and figures. Nor should there be a proliferation of redundant data, calling into question which set of duplicate numbers is right. There should be no egregious violations of MIS controls and standards that would permit security breaches, loss of resources, hindered migration or restricted integration.

Just because no damage is detected does not mean that end-user computing has necessarily been a success. It is possible that isolated uses of turnkey solutions have merit but that the wholesale promotion of end-user computing programs does not yield broad benefits.

To test the likelihood of this possibility, we will have to draw judgmental conclusions about the impact of end-user computing on organizations. It will be necessary to trust user observations of changes and impacts. We can determine the various degrees of end-user computing's success through the following sequence of questions:

- **Are users utilizing end-user computing techniques?** Normally, this is a terrible test because using end-user computing incorrectly can waste time and money and cause damage. However, for programs just getting under way, this is the key initial gauge of progress as well as a prerequisite for eventual payback. In environments in which there are high levels of hierarchical scrutiny, use is even more meaningful because it can indicate that the growing utilization of technology has, at least, passed a potential rigorous management review.
- **How are users utilizing end-user computing?** Eventually, ask this more exacting question to measure if the technology is being used beyond its rudimentary functions.
- **Have users met initial goals?** Failure to accomplish set goals might indicate that users are not serious about making the technology work.
- **Have users become more independent?** The indicators of independence include increases in inquisitiveness and independent action. Other behaviors to observe include positive responses to basic technology and an increased understanding of technological capabilities.
- **Have users become more efficient?** In viewing user performance, are there indications that they can accomplish their functions at a lower cost and with fewer resources? Attributing this efficiency exclusively to end-user computing may be as difficult as quantifying specific improvements, but it is one of the longer term predicted effects of the technology.
- **Have users become more effective?** Have improvements evolved to areas of quality, not just quantity? Has accuracy increased? Are users more knowledgeable about data, its meaning and its possibilities?
- **Has end-user computing changed users' behavior?** A final test is to see if personalized computing has altered the way end users work. For the promised potential of end-user computing to come true, jobs should eventually be considerably altered for the better by astute users who see the possibilities that technology can bring

Each of the previous questions can serve to confirm to management the degree of payback from end-user computing. These questions make up a hierarchy of tests that measure the impact of the technology and show increasingly higher benefits and paybacks. As we ask each question, we can learn that given time, greater benefits can, in fact, come about.

We can't afford to assume that these benefits will happen automatically. We must take steps to demonstrate current and future benefits at all levels to management and MIS through a methodical, increasingly rigorous analysis.

Young is managing director of MIS for the Wheeler Group, a division of Pitney Bowes in Hartford, Conn.

You're either safe or sorry.

CA-TOP SECRET™ represents a major advance in MVS and VSE security systems. Its comprehensive scope, exceptional auditing capabilities, intelligent design, ease of implementation and ease of use make it without question the system of choice over anything else available on the market today.

You get total security. And you get total support as well—on-site consulting and on-line HELP—and tutorials when you buy it as part of CA-UNICENTER™, the modular system designed to automate all data center functions. CA-TOP SECRET and CA-UNICENTER—total security within a totally automated data center. A complete solution and only Computer Associates can deliver it today.

Be safe instead of sorry. Call Dana Williams at 800-645-3003.

TOPIC V
DENVER CO
JUNE 10-12 1987
ORLANDO FL
JULY 26-31
1987 USER CONFERENCE

COMPUTER ASSOCIATES
Software superior by design.™

711 Stewart Avenue
Garden City, N.Y. 11530-4787

For Better Security
The way is CA

Circle Reader Service Number 51

© 1986 Computer Associates International, Inc.

Fill out and mail in the attached postage-paid envelope.

YES! I want to take advantage of this celebration offer . a full year of COMPUTERWORLD and the COMPUTERWORLD FOCUS issues for just $35, a savings of $9 off the basic rate Plus, I'll receive my FREE Magic Mug with my paid subscription

□ Payment enclosed □ Bill me

□ Charge my credit card □ AmEx □ VISA □ Mastercard

Signature ______________________ Card Expires ________

FIRST NAME M I LAST NAME

TITLE

COMPANY

ADDRESS

CITY STATE ZIP

Address shown □ Home □ Office

□ I'm already a subscriber but I'd like to extend my subscription at this special low rate (Attach mailing label above)

Canada Central & South America $110/ Europe $165/ All other countries $245 (Airmail)
Foreign orders must be prepaid in U S dollars

Please complete the information to the right to qualify for the special introductory rate

Basic Rate $44

COMPUTERWORLD

Detach here place in envelope and seal securely

Please indicate your business function and computer involvement below

1 BUSINESS INDUSTRY (Circle one)

10 Manufacturer (other than computer)
20 Finance/Insurance/Real Estate
30 Medicine/Law/Education
40 Wholesale/Retail/Trade
50 Business Service (except DP)
60 Government—State/Federal/Local
65 Public Utility/Communications Systems Transportation
70 Mining/Construction/Petroleum Refining/Agriculture
80 Manufacturer of Computers Computer Related Systems or Peripherals
85 Computer Service Bureau/Software Planning/Consulting
90 Computer/Peripheral Dealer/Distributor/Retailer
75 User Other ______________
85 Vendor Other ______________
(Please specify)

2 TITLE FUNCTION (Circle one

IS/MIS/DP MGT
19 Vice President Asst VP
21 Dir Mgr Supv IS/MIS/DP Services
22 Dir Mgr Supv of Operations Planning Adm Services
23 Dir Mgr Supv Analyst of Systems
31 Dir Mgr Supv of Programming
32 Programmer Methods Analyst
35 Dir Mgr Supv OA/WP
36 Data Comm Network/Systems Mgr

OTHER COMPANY MANAGEMENT
11 President Owner/Partner General Mgr
12 Vice President Asst VP
13 Treasurer Controller Financial Officer

ENGINEERING
41 Engineering Scientific R & D Tech Mgr

SALES
51 Manufacturing Sales Reps Sales/Mktg Mgr

OTHER PROFESSIONALS
60 Consulting Mgr
70 Medical Legal Accounting Mgr
80 Educators Journalist Librarians Students
90 Others ______________
(Please specify)

3 COMPUTER INVOLVEMENT (Circle all that apply)

Types of equipment with which you are personally involved either as a user vendor or consultant

A Mainframes/Superminis
B Minicomputers/Small Business Computers
C Microcomputers/Desktops
D Communications Systems
E Office Automation Systems
F No Computer Involvement

330567 9

news & analysis

UPDATE

Data crime laws passed

Legislation has addressed the world of information processing with two laws that protect users from unauthorized access and computer-related fraud. However, industry observers suggest that these measures are only a beginning.

The Electronic Communications Privacy Act of 1986 extends protection from eavesdropping on mail and telephone communications to include digital data communications such as electronic mail and remote computing.

The act also defines privacy for E-mail storage at off-site locations such as remote processing or time-sharing companies. These third-party rights protect the owner of the information from unauthorized access by government officials or employees of computing service firms.

The Computer Fraud and Abuse Act of 1986 makes it a federal crime to gain unauthorized access to data in any financial institution, federal government or interstate computer.

Crimes in which $1,000 worth of goods, services or dollars are stolen or software is destroyed are felonies with jail sentences of up to five years for the first conviction and 10 years for the second. All unauthorized access to medical data is a felony as well, regardless of price.

One problem with the fraud and abuse act is that unless stolen data is linked to a loss of goods, services or dollars, the theft is considered a misdemeanor, punishable by only one year in prisoo, says Jerry Marsh, executive vice-president of the computer security division of On-Line Software International, Inc.

Security issues at one of the world's most automated stock exchanges, page 16

To prosecute an alleged crime, Marsh states, the accuser must document the offenders' actions, placing the burden of proof for an invasion on the owners of the data.

However, the two security acts are a step in the right direction, according to the Data Processing Management Association (DPMA), an organization with nearly 45,000 members. But these documents do not deal with computer crime issues at the state and local levels.

In response, the DPMA has developed a five-part model computer crime act that covers the unauthorized use or access of computer resources, including any information stored on a machine; release of computerized information, copying or use of proprietary computer software and information and modification of computer resources; and denial of access to computer resources.

The DPMA has announced that it will work to identify states with weak computer crime laws and focus its activities on educating legislators and businesses so that laws are improved. Within these activities, the model computer crime act will serve as an educational tool.

Foreign exchange fraud cost VW up to $259 million

Erased and corrupted data reportedly contributed to a foreign exchange fraud that cost Volkswagen AG of West Germany up to $259 million. Company officials say they believe a fraudulent currency contract was created through transactions forged by changing computer programs and erasing data tapes in 1984.

Volkswagen has already filed charges of fraud, breach of trust and forgery against unidentified outsiders. Within VW, Chief Financial Officer Rolf Selowsky resigned in March, six weeks before his contract was to expire. Although Selowsky is not linked to the fraud, he has chosen to claim managerial responsibility.

The company has taken action against several high-ranking employees. Volkswagen has reorganized its finance division, dismissing VW's foreign exchange manager and suspending both its head of finance and payments and head of money and foreign exchange clearing for managerial failure.

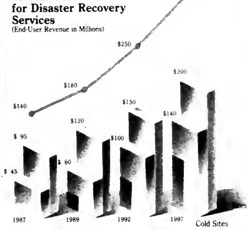
Financially, the fraud has widely affected Volkswagen and the West German marketplace. VW's stock price dropped 9.2% in the days following the announcement.

Other West German automakers felt similar losses, and

Continued on page 16

10-Year Forecast for Disaster Recovery Services

(End-User Revenue in Millions)



Information provided by International Resource Development, Inc

Fault-tolerant market to hit $2 billion in '87

The fault-tolerant market continues to be a two-man fight Both Marlboro, Mass.-based Stratus Computer, fnc. and Cupertino, Calif.-based Tandem Computers, Inc. have been sparring for some time to dominate the market, with IBM on the edge swinging but unable to land a solid punch.

The fault-tolerant arena is going to get a little more crowded. The traditional make-or-break markets, such as the banking and airline businesses, are now being joined by other industries eager for the extra security of fault-tolerant systems, which, in their basic makeup, contain processors working in parallel that continue to operate after componeot failures.

"We are predicting the [U.S.] fault-tolerant market will reach $2 billion in 1987 and grow 40% to 50% each year until 1990," claims Pete Kastner, manager of marketing development at Stratus. "Financial services, the brokerage business, point of sale [POS] and shop floor applications are exploding within business."

But International Resource Development, Inc., headquartered in Norwalk, Conn., sounds a more cautious note, pegging the U.S. fault-tolerant market at $1 billion this year, climbing to $1.2 billion by 1990.

"There are two big developments now under way in the fault-tolerant market," says Van Weathers, a director at Dataquest, Inc. in San Jose, Calif. "The first is expansion of target markets, which is bringing in some new vendors, and the second is the pressure being placed on the price/performance ratio. It's pushing the costs of transactions per second down."

Expanding markets, Weathers says, are exemplified by such new fault-tolerant frontiers as POS and telecommunications

"[fllinois Bell] is in the process of developing a system called Networker, which monitors telephone network functions, picks up operator-referred trouble reports, analyzes them and tries to pinpoint the problems," explains Rich Willer, manager of corporate networks and software support at Illinois Bell in Chicago. "The core of Networker is a [Parallel Computers Co.] fault-tolerant system with built-in battery backup. We can't have the system go down."

Willer explains that telephone companies have always, out of necessity, had fault tolerance but

Continued on page 14

Fault tolerant

Continued from page 13

not support systems such as Networker built into their switching systems. "Until now, our support systems really haven't had the transaction volumes and we only needed to have high availability not fault tolerance Increased competition is changing that." Willer says.

NCR Corp. has pushed fault tolerance into its bread-and-butter market, POS systems. At the same time, NCR is helping push the price curve down further with a series of low-cost, fault-tolerant POS systems in the $25,000 to $45,000 range, a far cry from the top-of-the-line Stratus and Tandem computer systems that can cost more than $1 million.

Tandem, however, has recently introduced a series of low-cost systems of its own, featuring an expandable number of processors.

Larger markets mean bigger competition. Santa Cruz, Calif.-based Parallel Computers is targeting its Unix-based systems at the telecom market as well as niche applications such as law enforcement agencies. New entrant Tolerant Systems, Inc. of San Jose is ambitiously aiming its low-cost systems at banking, telecommunications, manufacturing and the federal government — SK

Passwords made safer

A new class of security products has arrived that could radically improve the safety of password systems. These devices assign the user a personal identification number (PIN) every 60 seconds.

Passwords and PINs are the easiest methods of imposing some degree of data security on a system. However, they are also notoriously easy to crack.

Meanwhile, devices that force users to identify themselves via cards or biometric readings are much more secure — and much more expensive. They also require that user terminals be equipped with special hardware.

Now, however, a new kind of personal access device (PAD) has come to market. It consists of a pseudorandom number generator and a security system running on the host computer and other pseudorandom number generators in the possession of authorized users.

The host generator and the user generators are running the same algorithm, and both are running on the same clock. In other words, both the host's and user's systems are producing a new, unpredictable number every minute. But, it is the same unpredictable number for both of them.

Denied access

Users can then dial up the system on any terminal or personal computer they like. To access the system, though, they have to type in the PIN being shown, at that minute,·on their generator. If that PIN does not match the number generated at the very same minute by the host, access is denied.

Several products utilizing this principle have come to market — many of them the results of strategic alliances with one company, United Software Security, Inc., headquartered in McLean, Va.

Among other things, United Software Security sells Padpath, software that provides this kind of pseudorandom number access to IBM mainframes' security facility software, ACF2.

Currently, users can buy Padpath either alone or in association with proprietary hardware PADs from three different companies. United Software Security also sells Lazerlock, a small, hand-held user PAD. Another Padpath-equipped device is Confidant, from San Jose, Calif.-based Atalla Corp. This PAD is, in fact, a small calculator.

And, finally, Security Dynamics, Inc., located in Cambridge, Mass., recently introduced a smart card equipped with Padpath (see story page 52). — MT

Data Physician treats viruses

Imagine the shock of seeing text, perhaps hours of wbrk, oozing off the computer screen. At Apolln Computer, Inc., this occurrence is a rite of initiation for new employees, two engineers explain. The culprit is a program called Melt, which gives the appearance that the screen is melting away even though the data remains unharmed, the engineers say. It is a good practical joke.

However, some software has frightening effects that are more than just appearances; they are tools of software sabotage. Known as viruses, worms or logic bombs, these small strings of code either destruct or corrupt electronic data.

"Generally, only a small amount of code is oeeded to destroy software," says Barbara Hansen, president of Minneapolis-based Digital Dispatch, Inc., a software development firm. The virus checks for the time or other conditions, and when the proper conditions exist, she says, "the virus comes into play, wiping out data or scrambling disks."

A major problem for systems managers is that creating viruses is simple. "Anyone who has the wherewithall can do it," Hansen asserts. "It doesn't take much time, and it doesn't take a lot of intelligence." Thus, disgruntled employees have an easy form of revenge at their fingertips.

At the same time, searching for the minute defective code is akin to looking for a needle in a haystack. The problem is often compounded by the fact that the virus can come into a system through external means, such as electronic bulletin boards or micro-to-mainframe links, which are hard to track.

Disastrous results

The cnnsequences of these viruses can be disastrous. In early 1985, a time-sensitive logic bomb froze all the internal files residing on an IBM mainframe at the Los Angeles department of water and power. The department did not have to curtail its utilities services, but it had to bring the IBM machine down for a week to remove the bad code, Hansen recalls.

While the incident was a source of frustration for the utilities department, it was inspiration for the engineers at Digital Dispatch. "After reading about the L.A. logic bomb, we felt there was a need to develop a product that would catch the virus before it activated," according to Hansen.

In 1985, the firm introduced Data Physician, a $49.95 package for PCs that reportedly locates and helps remove viruses. When the PC boots up, the product works by monitoring files that have been listed by the user, Hansen explains. If the file is corrupted, Data Physician gives the operator the option to back up the original.

One weakness of Data Physician is that the waiting time for the file check is noticeable, Hansen says. The company plans to offer a second virus-checking package that skirts this problem, however. "The software will be attached to the front end of each file so that it checks the file every time it's used," she says.

Beyond Digital Dispatch's products, users have few commercially available alternatives.

Instead, managers need to monitor and regulate the use of their computer systems "The best thing to do is limit the software that users can introduce to the system," says Sanford Sherizen, president of Data Security Systems, Inc., a Natick, Mass.-based consultancy.

Managers should also restrict who can make changes to the software and who can sign on, he says. — RH

Lock or shred your data cares away

Most vendors and users think of data security in terms of electronic security. But, the physical protection of data that is io the form of paper or magnetic media cao be every bit as important and far more difficult. MIS is paying increased attention to physical defense measures — safes and vaults that secure data and shredders that destroy data

Buying such devices is not easy. Data safes, fnr instance, are not just born-again bank vaults converted to data storage The protection of data is a very different thing from the protection of money. A coin, fnr instance, is not likely to suffer destruction because of humidity or magnetic fields.

Even fireproof safes, which were designed to protect paper records, are not necessarily what a firm needs. Paper is much tougher than disks or tapes. While paper will easily survive temperatures of 350 degrees Fahrenheit, most magnetic media will melt at 125 F to 150 F Likewise, paper can stand high levels of humidity, but magnetic media perishes in the area of 80% to 85% humidity

When purchasing a data safe, MIS officers should, therefore, make certain it meets the Underwriters Laboratories, Inc. (UL) standards for the protection of magnetic media. The level of protectinn required for the protection of diskettes is UL Class 125.

Underwriters Laboratories tests safes by locking them and placing them in a furnace. The furnace is then fired to 1,700°F and left on for one bour nr more, depending on the type of safe Next, the furnace is switched off, and the safe is allowed tn cool, in the oven, for a period of 45 hours. If, during that time the internal temperature of the safe exceeds 125°F or the humidity exceeds 80%, then it is not awarded UL Class 125 status.

Several firms market safes at UL Class 125 nr above. Schwab Safe Co., in Lafayette, Ind., offers a line of data safes ranging from desk-side models to The Monster, a strnngbox nearly the size of a bank vault.

However, along with pondering the protection of data MIS should also think about the destruction of data. In an age of disk drives and high-speed printers, industrial espionage can be nothing more complex than the theft of a disk or printout

MIS officers must therefore, include in their data security calculations shredders and other devices that prevent wastepaper from falling into the wrong hands Fortunately, there is an entire shredder industry eager to be of service

Things to consider when buying a shredder include the sort of media you want to destroy and how completely it must be rendered unreadable If you are only dealing with single sheets of sensitive, but not critical, material a desktop shredder may be all ynu need. But if you must destroy whole printouts, microfilm, magnetic media or even printed-circuit boards, you will need industrial facilities

MIS will also need to consider how completely it needs waste broken apart A simple shredder, which reduces a document to a collection of strips, is inexpensive and effective, but it may not be totally secure. A sufficiently dedicated enemy can paste together the strips

Reduced to powder

If your data is particularly sensitive, you may wish to invest in a device that reduces paper or other media to a fine powder One firm that makes such machines is Security Engineered Machinery, Inc. (SEM) in Westboro, Mass This company markets devices known as "disintegrators."

An SEM disintegrator contains a cutting chamber in which paper, reels of microfilm, magnetic tape, floppies and the like are ground apart by rotating blades. The waste fragments only leave the chamber when they are small enough to be drawn through a wire mesh — the size of which can be varied depending on your security requirements.

SEM machines can be used to destroy just about any piece of paper, plastic or soft metal that can pose a security problem The disintegrators will even swallow typewriter ribbon and circuit boards Currently, most of SEM's customers are government agencies, government contractors and American diplomatic services, which have disintegrators in U S embassies around the world — MT

Feds look to secure ports through Tempest

The Tempest security program has been in existence now for more than a decade and is enjoying its best business ever. Top U.S. computer manufacturers such as IBM, Digital Equipment Corp. and Wang Laboratories, Inc. have been offering Tempest-certified workstations for several years, spending a great deal of time and money shielding their equipment in order for their computers to undergo extensive National Security Agency testing before they are stamped Tempest-approved and placed on the government's Preferred Products List.

Who buys these machines? Russ Aldrich, manager of Communications and Special Systems at San Jose, Calif.-based Altos Computer Systems, Inc., one of the newer Tempest vendors on the block, says there are a number of government agencies that handle classified information and require Tempest equipment. Users include such heavyweights as the Department of Defense, the Federal Bureau of Investigation and the Central Intelligence Agency.

"[Altos] thinks that the U.S. Tempest market will triple in the next three to five years," Aldrich claims. "Tempest only represents one of three primary hardware security options now available. There are also embedded computer systems that go into ships and airplanes and electromagnetic pulse [EMP] systems, also called EMP-hardened systems, that are geared to withstand indirect nuclear blasts. While EMP systems prevent radiation from coming into the systems, Tempest keeps radiation emissions from getting out."

Computers meet politics

The Tempest process involves eliminating electromagnetic emissions (usually through lead shielding), produced by all automatic data processing equipment, that could be illegally monitored and deciphered. Tempest is one nexus where computers, politics and espionage meet.

Security also has a price. Aldrich says that Tempest-certifying a system will roughly double its final price. It can also take a vendor years to produce a machine that, in the end, might not pass strict government Tempest testing, a process that can take up to three months

"But Tempest spm-offs, especially in software, are opening new markets," Aldrich says. "A government-designated security measure called C2, which is built into software and provides a lower level of user access security, is already getting a good deal of attention from private industry."

Software security, such as C2, which Aldrich says will show up in commercial products within a year and a half, and its more stringent security relative, B1, are set forth by the U.S. government in accordance with criteria in the Trusted Computer Criteria. This volume of criteria is issued by the Defense Department's National Computer Security Center.

Could Tempest eventually invade the commercial sector?

"If you consider Tempest as just one of several possible security measures a company could look at, then Tempest could make some individual sales," says Ed Clough, associate manager of public relations at Wang

Meanwhile, the number of Tempest vendors whose products are listed on the U.S. government's Preferred Products List is growing.

Systematics General Corp. of Sterling, Va., has used Apple Computer, Inc.'s Macintosh computer to produce a Tempest-certified desktop publishing system; VCA Corp. of Reston, Va., has introduced a Tempest-approved supermicrocomputer that runs Unix; and Convex Computer Corp. of Richardsoo Texas, has announced a Tempest variant of its C-1 supercomputer.

In the communications area, Wang and other companies are working on Tempest-secured local-area networks. — SK

The security of securities

Electronic stock exchanges may make fraud harder to detect

International currency, stock, bond and future exchanges have gone electronic with a passion in the last few years. Increasingly, the business of securities exchange has become a high-tech operation involving computers, data links and other aspects of an information-based industry.

In the process, though, the international securities trade may be becoming increasingly insecure. Some analysts worry that a few thieves could exploit the sheer speed and flexibility of global trading to conceal fraud on a vast scale.

"What concerns me most is 24-hour trading," says Jack Bologna, president of Computer Protection Systems, Inc., security consultants. He notes that some stock exchanges are now trading 24 hours a day. This is to the exchanges' advantage because it lets them woo customers in every time zone on the globe

But, Bologna says, this situation also means there is no time when the exchanges are forced to shut down and take account of what has occurred that day "Huge amounts of fraud and embezzlement could be disguised as daily float, for instance," he says.

Yet this scenario does not even begin to address the problems securities dealers have when they attempt to keep their data and communications lines free from unwanted listeners.

Some industry observers now believe that the only route to security is for the stock exchanges themselves to become guardians of securities transactions.

For instance, one of the most automated exchanges in the world is the Cincinnati Stock Exchange. It is a little-known but vigorous exchange, gradually stealing business from both the American and New York stock exchanges.

Its setup is completely computerized. It has no trading floor, no human brokers, no ticker tape machines or big board. Instead, the operation consists of a vast room filled with fault-tolerant computers. Dealers and brokers, sitting in the comfort of their offices across the country or the world, trade via electronic links.

"You can't break in, at least, not via dial-up access," notes Cincinnati Exchange President K. Richard B. Niehoff. Member brokers are connected through dedicated lines. And, he says, "There's no traffic on them but ours." The data on those lines is encrypted via an algorithm that is probably proprietary to the exchange, but even that data is classified.

"Of course, someone could walk into one of our members' offices, sit down at a terminal and start making trades," Niehoff says. "But that's rather easy to detect. A stranger doesn't drop in off the street without attracting some attention."

He notes that while these sort of precautions won't eliminate the possibility of fraud, they can reduce it to manageable levels. He notes, for instance, that the exchanges know their members and know when someone who isn't a member is getting into the system.

Still, precautions work only when the exchanges are willing to take them. MIS already knows too well the long and bitter struggle to enforce even basic levels of security on far less vital information.

Ultimately, though, the computerization of stock exchanges is probably unstoppable. The software developed by the Cincinnati exchange is being widely remarketed in Europe. Meanwhile, those exchanges that have already gone electronic have been roaring successes and ghost towns overnight. "If you look at the London exchange," Niehoff notes, "you'll see the floor has become just about empty." — MT

dB

By Rich Tennant

OH HI. I'M GLAD YOU GOT HERE EARLY. THIS TIME THE DATA SECURITY ISSUE ISN'T GOING TO GET SHORT CHANGED IN THE BUDGET.
I UNDERSTAND THE RESISTANCE TO EXPEND MONEY FOR SOMETHING THAT HASN'T HAPPENED YET, BUT WITH THE NUMBER OF LOGIC BOMBS, WORMS AND VIRUS CODES, YOU CAN'T TAKE A WAIT AND SEE ATTITUDE.
I THINK THE ONLY WAY TO IMPRESS THE IMPORTANCE OF PROPER DATA SECURITY IS TO DRIVE HOME THE POINT OF VULNERABILITY, WHICH CAN STRIKE WITHOUT WARNING AT A MOMENTS NOTICE.
NOW HELP ME RESET THE PAIL BEFORE THE OTHERS GET HERE.
CONFERENCE

Update

Continued from page 13

the Commerzbank index dropped 28.3 points.

Prices have since begun rising. However, the fraud will have longer term effects on Volkswagen; the controversy has put a hold on West German government denationalization plans to sell its shares of VW stock.

U.S. fears foreign powers will access public data

Former National Security Adviser John Poindexter's "sensitive but unclassified" directive, which gave the government power to monitor and censor private data bases, was rescinded in March. However, the U.S. administration is still concerned about foreign access to public information.

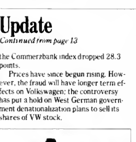
This fear stems from such data as that gathered in a 1985 status report from the National Telecommunications and Information Systems Security Committee. That report quoted KGB defector Vladimar Sakarov as stating that "the KGB routinely accesses credit agency data bases in order to find persons working in defense industries who are in serious debt."

The implication is that people in debt would be the most willing to trade national secrets for cash with the KGB, the Soviet secret police and intelligence agency.

The Soviet Union as well as other countries continue to have access to these data bases, in part because Poindexter's directive was rescinded. Businesses, legal experts and the administration agree that the directive had to be repealed because it overstepped the boundaries of power set by the U.S. Constitution.

However, the rescission of Poindexter's directive has sent government security officials back to the drawing board to try and determine a means of protecting this type of information from foreign governments.

News section compiled by *Computerworld Focus* staff members Stan Kolodziej, Michael Tucker and Rebecca Hurst.



PRODUCT ANALYSIS

Security in the first degree

BY MICHAEL TUCKER

For a while, data security was a relatively simple problem with a relatively simple cure. MIS just took the mainframe, plus the assorted tapes that ran on it and locked it all in the data center. For a slight additional investment, MIS could even obtain an intelligent user authorization subsystem — an armed security guard.

Then came distributed processing, global networking and the personal computer with attached modem. Suddenly, data security became infinitely more complex. Sensitive information could be accessed now by any number of systems scattered across any number of locations using any number of different communications lines.

"With every new product release, you get problems," explains Steve Josselyn, a senior analyst with consultancy International Data Corp., located in Framingham, Mass. "Technology is just running so fast that the ways to secure things haven't kept up."

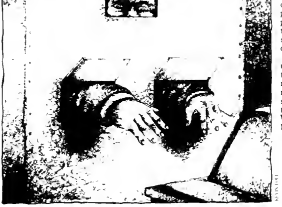
Happily for MIS managers, however, several security options are becoming available. They range from sophisticated encryption algorithms to biometric user identification devices. Data security specialists say that matching the right solution to the right problem is now the second greatest data security challenge for MIS.

The most pressing challenge, the security experts say, is making upper level, non-data processing management aware that the problem exists.

Ultimately, the choice of security apparatus depends on how sensitive the information is. If the data is of relatively little value, the system is a centralized machine, users are almost entirely on in-house terminals and security requirements are small, then a simple password system with multiple levels of access is all a company needs.

However, recommending passwords is next to saying the company will have no security system at all. Password systems are like white picket fences and "Keep Off the Grass" signs; they depend on the cooperation of the very people they are supposed to restrain.

Many MIS people report that their biggest concern is not hackers, but legitimate users who wander into places where they're not supposed to be. "We just can't afford unrestricted connectivity," says one MIS officer at a Wall Street investment firm. "End users can mess up data files — maybe even their own pay records — by accident After we point out that bit about payroll, we get lots of cooperation from end users "



For some situations, passwords are quite workable. But, MIS should never lose sight of just how insecure passwords really are, particularly if the system involved has the slightest capacity for dial-up access.

"People will insist on using a password that's taken from the dictionary," warns John Carroll, a professor and a specialist in data security at the University of Western Ontario in London, Ontario.

Tucker is *Computerworld Focus's* features editor

PRODUCT ANALYSIS

"There are programs available that dial up the system repeatedly, trying every word in the dictionary, until finally they get it in. It may take days, but, ultimately, they crack the system," he says.

Carroll notes that fairly easy measures can increase password effectiveness dramatically, such as using upper- and lowercase in the password rather than just simple ASCII characters.

MIS can also increase the security of its systems by investing in products that allow greater management of dial-up access. Telco Systems Corp., headquartered in Natick, Mass., offers a product known as the Network Administrator. Running on a PC, the product can enforce password use, keep a complete audit trail of network traffic, yield a call-back function and provide for encryption. The company says that a Network Administrator-governed network can be installed for less than $1,000 per host port.

Dialing for dollars

Once people access the mainframe by phone, MIS's security problems are vastly increased. Few, if any, means of communication are easier for a dedicated thief to tap than the telephone line.

But there is no guarantee of safety even if, by some miracle, MIS manages to enforce a ban on dial-up access. If a machine is doing any sort of networking at all, MIS can usually assume that somewhere along the line there is going to be a leak. In an age when communications managers will use multiple channels of communication — routing data around failed nodes or switching carriers at a moment's notice to take advantage of reduced prices elsewhere — networks leak like sieves.

Even if a company is not networking at all, its data is still not safe. It has become all too easy to listen in on computers via their electromagnetic emissions. So ultimately, it is best to assume that nothing is secure. And if a company's data is of any value at all, it is best to encrypt it.

Currently, the encryption world is divided into two groups — the National Security Agency (NSA) Data Encryption Standard (DES) partisans and those who choose offerings from independent organizations.

DES has been *the* security algorithm for almost a decade. It is so hard to crack that it was adopted by the supersecret NSA as well as the American banking community. Today, most encryption products on the market make use of DES in one form or another.

However, the future of DES is unclear. The NSA recently announced that it had qualms about DES and that it was working on its own set of algorithms. These new, more secure algorithms would remain the property of the NSA, but the government would make them available to developers in the form of sealed chips. Vendors could then integrate these chips into their systems.

DES users and vendors objected to this course of events. The American Bankers Association, for instance, led the fight to give DES a stay of execution. After a brief but energetic contest, the government agreed that DES will continue to be a standard in the commercial world. However, the NSA will also continue work on its own set of devices for use in national security applications.

Meanwhile, MIS can exploit DES. No matter what its eventual fate, DES remains one of the most secure encryption methods. To date, no one has reportedly broken it.

DES-based systems are widely available usually directly from large hardware vendors. Most computer makers offer DES encryption as an option on their boxes. A number of third parties offer it as well. Ideassociates, Inc. in Billerica, Mass., for example, offers Disket 2 Plus, a removable hard disk with DES encryption for the PC. When the disk is not in use, a user can simply remove it from a machine and lock it in a safe. If the disk is stolen, the data still cannot be read without a key. Disket 2 Plus is priced at $3,595.

In the event that MIS does share some of the NSA's concern about DES, it can either write its own encryption algorithm or go to an independent supplier such as RSA Data Security, Inc. in Redwood City, Calif. "We are the only private competitor to the NSA as a supplier of cryptographic algorithms," claims D. James Bidzos, RSA's vice-president.

An algorithm alternative

The heart of RSA's product offerings is the RSA algorithm, named after company founders Ronald Rivest, Adi Shamir and Leonard Adleman, who developed it while they were professors at MIT in 1977. In some ways, RSA is actually more secure than DES itself. For example, RSA allows the data recipient to verify the sender via special data "envelopes."

Currently, RSA licenses its algorithms to both hardware and software vendors. Otherwise, a company can purchase it directly from RSA in such products as Mailsafe, a PC-based product that costs $250.

If a company requires further data security, it can try to control user access. In practice, this control usually translates into a system whereby users receive a unique personal identification number (PIN), ID card or the like without which they cannot access host data. The classic example of this security arrangement is the automatic teller machine, which prevents transactions without the user presenting both a PIN (in the form of a password) and a bank card.

Requiring PINs is an inexpensive and

easy way of beefing up security. Unfortunately, because PINs are only upgrades of traditional passwords, they can also be insecure. Therefore, most vendors combine PINs with some sort of hardware users must attach to their systems or terminals.

For example, Leemah Datacom Security Corp., located in Hayward, Calif., offers the Tragnet Secure Call-In Device (SCID), which brings a hardware/PIN combination to dial-up networks. When a Leemah product, Tragnet 2000, is installed on the host, an end user must have a Tragnet SCID and a PIN to gain access. The user dials in the PIN, and the 2000 identifies the number and sends back a challenge code. The SCID then returns a DES-encrypted response. If everything matches, the user can access the system.

Meanwhile, the hardware user ID devices getting the most attention right now may be smart cards and smart card readers. Smart cards are similar to credit cards except that they contain a considerable chunk of information about the user.

Some smart cards contain a small microprocessor plus attached read-only memory. However, there are other technologies vying for the smart card role. Drexler Technology Corp. in Mountain View, Calif., has been promoting Lasercard, an optical memory card system.

> **In an age when communications managers will use multiple channels of communication — routing data around failed nodes or switching carriers at a moment's notice to take advantage of reduced prices elsewhere — networks leak like sieves.**

There is, however, one common drawback to passwords, PINs, smart cards and encryption keys: They can be stolen.

If a company's data is very important, the firm may wish to investigate biometric ID devices. These machines identify users by some physical feature that is almost impossible to duplicate, such as fingerprints or voice patterns. "Generally speaking, the best solution is something that's personally unique to the user," says Jack Bologna, president of security consulting agency Computer Protection Systems, Inc. "Something that is part of the user is about as personally unique as you can get. Some of the experts talk about biometric devices as being the ultimate in user access control."

At the moment, biometric ID devices have their share of development problems. All but the highest end systems, for example, suffer from high error rates. Bologna thinks it will be five years before "biometric devices are tolerably perfected. I think a 90% to 95% recognition rate is about the best we're going to manage."

Still, for the MIS officer whose data simply must not be stolen, biometrics hardware may be the best bet. A number of companies currently offer systems that might be either directly attached to user workstations or merely used to keep unauthorized personnel out of DP areas.

Fingerprint recognition systems can be obtained from vendors such as Fingermatrix, Inc., of N. White Plains, N.Y., and Indentix, Inc., of Palo Alto, Calif. Each firm provides terminals that can quickly identify users by comparing an electronic reading of a user's fingertips with a template stored in a system memory. The Fingermatrix product costs $3,500, while the Indentix product costs $5,000. Indentix is working on a version of its product that would fit into a PC's expansion slot.

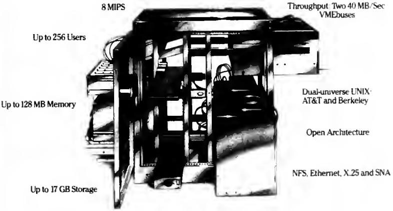
Another biometric approach is retinal identification. Eyedentify, Inc. in Beaverton, Ore., offers a series of devices that scan a user's eye with an infrared light and attempt to match the pattern of blood vessels in the individual's retina with a stored image. Eyedentify's systems are very high end; they cost between $6,000 and $7,000 and are very secure.

It is thus possible to use a combination of PINs, cards, encryption and biometrics to produce a security system that would put Fort Knox to shame.

But if that system is not matched by a commitment to security on the part of upper level management, it will be totally useless. "Let's assume you have a secure system," explains Charles E. Perkins, security supervising consultant with Baltimore-based Coopers & Lybrand. "What do you [the business executive] do with the data? Well, you print it out. Then, you stick it into an interoffice envelope that is secured with nothing more than a string, and you hand it to a mail clerk who's paid the princely sum of $3.50 an hour."

His point is simply that data security is not, strictly speaking, an MIS problem. It is a corporate problem. The theft of data is, in the end, no different than the theft of any other company asset. "Senior management is only now becoming aware of the fact that they've got a strategic asset in data," Perkins notes.

The challenge for MIS is to make the security issue clear to employers who, through simple carelessness, may be the far greater threat to data than whole armies of hackers. But, Perkins admits, "it's a tough sell." ❖


8 MIPS
Throughput: Two 40 MB/Sec VMEbuses
Up to 256 Users
Dual-universe UNIX: AT&T and Berkeley
Up to 128 MB Memory
Open Architecture
NFS, Ethernet, X.25 and SNA
Up to 17 GB Storage

A new vigilance

Security has piqued the interest of MIS and management at all levels

BY STAN KOLODZIEJ

As if MIS managers don't have enough work dealing with applications backlogs, fielding user complaints and grooming themselves to become chief information officers, they must also shoulder the growing chore of computer security.

Safeguarding systems is no mean task. Computer security runs the gamut from individual passwords and data access controls to multimillion-dollar disaster recovery plans. MIS has done its homework throughout the past decade trying hard to convince senior-level management in corporations that securing the data center is not just important to their businesses — it is critical.

"The selling job is paying off," explains Charles Perkins, a supervising consultant with the Management Consulting Services division of Coopers & Lybrand, located in Baltimore. "More businesses have become aware of just how dependent they are now on the computer. If the computer is not the brains, it is certainly the heart of most corporations. As the computer goes, so does the business. It's given a sense of vulnerability to a lot of companies."

That sense of vulnerability, combined with some recent, well-publicized computer-related disasters, has drawn more senior managers into the security picture.

"That whole attitude — upper management telling MIS they really don't know what MIS is doing and don't want to know as long as the reports are getting out — has changed," says Jack Bologna, president of Computer Protection Systems, Inc., in Plymouth, Mich. "It's too important now not to know about the data processing side."

Senior management's attitudes toward security are changing, agrees Jim Finch, president of Cerberus Computer Security, Inc., a Toronto data security consulting firm. "Each year, top management seems to become a year younger as a new generation comes in I wouldn't say that the new generation is obsessed with security, but they are probably much more computer literate. And in that computer literacy, one of the slots is security."

There are other factors prompting top management to sit up and take notice of computer security. The U.S. government has legislated security laws in the banking and savings and loans industries, two key U.S. businesses. In 1983, the Comptroller of the Currency and Administrator of National Banks passed a federal law that all national banks must have a disaster recovery plan in place. In 1986, the Federal Home Loan Bank Board declared the same stipulations for U.S. savings and loan institutions.

"These are important, high-profile industries," explains Nancy DeMatteo, vice-president of education at HSH, Inc., a Dublin, Ohio, computer security consulting firm. "[Security] is a big issue. The government has deemed it important enough to step in and take action. By doing so, it has declared computers critical not only to these businesses but also to the U.S. economy in general. It has caught the attention of MIS superiors."

At Irving Trust Co. in New York, the federal

Kolodziej is *Computerworld Focus's* senior editor banking security law helped underline what Walter Hill, senior hardware planner for the bank, describes as an already major concern within the company

'We've never had to hit management over the head about security.' Hill explains. "Our risk management group oversees information systems security and is always talking to senior management. What we have is a concerted security effort between the information systems grnop. internal auditors and the corporate risk management group."

The selling job has paid off, bot the flip side of extra security measures is a heavier work burden fnr MIS. In some cases. MIS seems to have taken a security tiger by the tail

"It gets toogher every day," Hill admits. "It's a lot of work and planning, and that's not all. We re nnw using some nf nur smaller computers to develop disaster recovery plans for our foreign brancbes. We have to. It's considered critical because nur business is so international. Though our contingency plans are broadening. I'm still the only one who does it. With MIS staffs cut back. it gets even harder," Hill says

Joe Wholley. manager of MIS evaluations at Borg-Warner Corp., a Chicago-based cnnglomerate. describes his firm's special security needs. Wholley says Borg-Warner is basically a series of autonomous operating divisions. and althoogh two of the company's divisions have opted to contract with outside consulting firms for help in computer security planning. other divisions and headquarters have handled much of the final formatting and installation of security plans themselves. There is a balancing act between corporate and divisional security objectives

"Our plan bad two parts," Wholley explains. "MIS first tried to get all the logistics in frnm various divisions about numbers of equipment, kmds of personal compoters and software applications and so on Next, we got management [at the divisions] to identify the kev osers of these systems. To help, we sent them a seven-page questionnaire

The selling job has paid off, but the flip side of extra security measures is a heavier work burden for MIS. In some cases, MIS seems to have taken a security tiger by the tail.

"Sitting down with the division managers and key users, we reviewed tbe [questionnaire] results and then started to understand how moch interdependence there was among the various departmental groups and divisions, how much the recovery of these systems would involve and what the effects would be on these users to be withoot computer service."

Next, Wholley had key users sit down and prioritize the following: how soon they woold need a recovery service; what it would involve for them to do their work on a manual basis if necessary; and, if they opted for a stand-alone backup system on a microcomputer, what files were crucial to business and what applicatinns would need to cnme up first should a disastei occur.

"These key users were the uoes who ultimately derived what the ootage and recovery periods would be," Wholley explains. 'Although the initial logistics involved a general fill-in-the-blanks approach, I had done data center reviews at every one of the divisions and knew their operations fairly well enough to tailor their security to some degree. In the end, ose was highly individualized because each location had a different set of demands that were met. Bot it's their responsibility to pot their own plans in motion."

Though moch of the attention has centered on physical disasters such as floods, fires and computer crime, computer security is widening its contents. The spread of PCs as stand-alone devices, as parts of local-area and long-haul networks and as devices plogging into mainframes is causing security headaches for MIS.

"There's one organization in the Chicago area that recently conducted a study to see how many PCs it had hanging around," Coopers & Lybrand's Perkins explains. "The firm discovered it had more money invested in PCs than it had in the data center."

Perkins adds that the entire area of PC controls is of major cnncern right now "Yoo have the question of PC data security, the qoestion of compatibility, standardization and so on, and I'm not sure that opper level management really understands this. It's too abstract. It doesn't seem as immediate and as real as disasters," according to Perkins.

Cerberus Compoter's Finch agrees. "The hot security topic these days is the PC. largely becaose so many people are learning about PCs for the first time. Downloading [data] is a big concern, but it's really not so much of a security prnblem as it is a matter of trust and personnel management."

Finch adds: "I don't think MIS is doing much of a job in educating its users on the secority procedures and implications of PCs. I think the user departmeots are making more use of nutside educational facilities. There are consulting groups now that teach security procedures all the way through the corporate pecking order. Tbey are running security conferences on a continual basis."

Bologna of Computer Protectinn also says he feels the end-user community is not getting adequate instruction from MIS on a variety of security concerns. These concerns range from passwords to the impact of PCs and departmental-level data bases to the reason for the various levels of access secority.

"I guess the fault should lie with those people who know the most about it, that is, MIS," Bologna explains. "But MIS is already onder a lot of pressure. I also think tbere's a feeling among MIS personnel that they are doers, not teachers. They'll leave that to others."

Companies such as HSH and Computer Protection Services have taken up much of the slack in educating users about corporate security procedures.

"A majority of companies will send employees to security conferences and seminars," HSH's DeMatteo explains. "What we try to provide [through educatinn] are user methodologies for their own security plans. [This edocation is] not just for end users bot for senior management as well. Security plans are more corporatewide now, not just focused on the data center."

Some companies already have an inside educational resource: information centers.

"We use the information center to handle some of the security education when MIS is overburdened," Irving Trust's Hill explains. "We feel that the only way you know you have a workable plan is to go out and test it And the only way you know that your people understand their responsibilities is to have an ongoing presence. That's why we test all the time, get the people involved, and that's the way we gain a confidence level that what we do would work in a disaster."

Finch claims, however, that Irving Trust's case is atypical. "Rarely are there enough skills in the client company to cover edocation," Fincb says. "Companies osed to come in and do short, snappy [security] assignments, do a security review and often provide some instruction."

Security tasks grow

The security task checklist continues to grow for MIS. Computer technology and increased bosiness competition is putting more stress on communications and on-line transaction processing. With this emphasis comes a need for devices such as fault-toleraot systems.

"It's not jost the traditional companies such as brokerage firms, banks and airlines that need faolt-tolerant systems," explains Charles Caswell, president of Caswell Systems, Inc., a Hudson, Mass., developer of a disaster-tolerant computer techoology. "More and more companies are beginning to put their computer operations on-line. They are beginning to move away from the batch environment into one in which on-line data is of eqoal importance or of even more importance than batch data.

"In this kind of environment you have to constantly maintain the integrity of the data files," Caswell says. "The system has to be available and up all the time. As more people are saying, 'We certainly need fault tolerance,' they are also saying, 'We also need some sort of disaster recovery plan.' They are tending to see these two as separate entities. In reality, thoogh, if they step back a bit and think aboot them as one entity, they can achieve both goals."

According to Perkins, security consulting firms are fast becoming essential third-party players in dealings between MIS and disaster recovery firms.

Unique solutions

"There are a nomber of different philosophies on business continoity planning. There are numerous cookbook, fill-in-the-blanks contingency planning products on the market," Perkins claims. "The fact is every organization has some things that are uniqoe to it. Two firms in the same industry with the same hardware and software probably will not use identical solutions because of the business philosophies of the organizations.

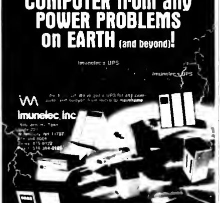
"I feel consultants are more objective and can provide a more customized approach tn computer secority," Perkins says. In addition, consultants can save customers money. He says that his group is often called in to go over client contingency plans and look for overlap and waste.

Finch is not so convinced. "There's always a fundamental checklist of security things to cover first in any organization," he says.

"Consultants always look at their competition in the business place as perhaps osing more mundane techniques than they are. Any consultant, however, is going to tell you that they use unique techniqoes for unique problems."

However, Perkins insists on the necessity of a neutral party who can come in and not get involved in the client's inevitable political problems. "Yoo go to an organizatioo and ask a user if his application is critical. If you don't do it in a structured and thought-out way, what [else will] users say but, 'Of course I'm critical. If I'm not critical, why am I here?' Yuo have to be above the political pulls."

Bologna says he agrees that most MIS can use outside help in security matters. "One of the problems MIS has to fight is the conception by upper management that MIS can do anything," he says, "and that often applies to computer security as well. [Outside aid] can help, but you can't just throw money at a security problem and expect everything to be cured. Most of it is still going to fall on the shoulders of MIS." ❖



Are you doing anything?

A Big Eight firm's computer security survey results

BY TONI B. FISH

While managers realize the benefits of computers, it has been only recently that they have begun to recognize the flip side of computerization — the dangers associated with breaches in computer security.

For many years, information security was almost exclusively a concern of military-related organizations and the banking industry. Now, in many kinds of business, when senior executives evaluate the caliber of their organizations' information systems, they see effective security as the popular new kid on the block.

This trend is evidenced by a computer security survey conducted in November 1986 by Ernst & Whinney, a Cleveland-based international management consulting, accounting and tax advisory firm (see story page 24 for survey methodology and respondent profile). The survey revealed that the maintenance and care of computer information are of vital concern to senior management.

Eighty-seven percent of the survey respondents indicated that their companies recognize the increasing importance of security issues (see chart this page). However, only 6% of the respondents said their organization's safeguards against security risks are completely adequate. These results demostrate that there is still a gap between security awareness and implementation.

This gap is not unique to security; often, when an organization's senior management recognizes a new concept, middle management needs time to develop a structure or procedure to accommodate that idea.

Safe and sound

An Ernst & Whinney study reveals an increasing level of concern for security among MIS professionals

- **87%** recognize security's importance
- **75%** are implementing security policies
- **62%** see security risks rising
- **42%** have security orientation for new employees
- Only **6%** say security safeguards are adequate

For example, 62% of the respondents said they believe security risks are rising, and 75% are taking steps to implement security policies. Less than half, or 42%, of the organizations surveyed have information and computer security orientation programs for new employees. So, while awareness and concern about security issues are increasing, survey respondents recognize that the actual safeguards organizations implement are not meeting these concerns.

The survey identified other major security issues, including the following:

- Data protection from the competition and employees.
- Priority of data classification, network security, microcomputer security and contingency planning.
- Continuity of service.
- The impact of the National Security Decision Directive 145 (NSDD 145). NSDD 145 was signed by President Reagan in September 1985. The directive established national policy concerning the telecommunications and information systems security of government contractors.

The respondents identified their competition, employees and foreign governments as the primary groups from which they want to protect their organizations' data. They also cited suppliers, customers and public interest groups.

Respondents from government and nongovernment organizations had differing opinions about which group was more important.

Fish is codirector of Ernst & Whinney's information security services practice in Cleveland.

Business and industry identified their competitors as the most important group from which they must protect their data. Government organizations cited foreign governments as a top-priority threat. Protection of information from employees ranked second for both government and industry

Historically, the security perspective grew from the audit perspective. That is, organizations considered internal, unauthnrized access to critical information by employees as their major security threat The emergence of competition as a computer security concern is a new trend. Reasons behind this trend include the increased computerization of strategic information and organizations' recognition that this information and effective automation provide a competitive advantage

Priority issues

Respondents identified data classification, network security, microcomputer security and contingency planning as the primary security issues currently facing government and nongovernment organizations. Given that data classification is required of many government agencies, it is not surprising that more government respondents than nongovernment respondents listed data classification as a priority issue. It is surprising to note, however, that this issue was not even mentioned by respondents in a similar Ernst & Whinney security survey last year.

Network security — last year's top priority issue — was mentioned frequently by both nongovernment and government organizations. While the survey did not define it, oetwork security usually includes protection of computer networks and computer applications from authorized and unauthorized users, message confidentiality and integrity and end-user authentication. End-user authentication will continue to be a focus of security efforts as the processing environment becomes more complex and as user identity grows more difficult to verify.

To meet the current and future demands of network security, the use of encryption will increase greatly, according to Ernst & Whinney. Increased networking will require new methods to ensure confidentiality and integrity based on encryption technologies for telecommunicatinns, file storage and message authentication.

Both surveys targeted microcomputer security as a major issue. Although the surveys did not specifically define the term "microcomputer security," a general interpretation includes microcomputer protection as property; applications protection from outside interference or contamination, and data protection, whether stored therein or nn associated storage media, from modification, destruction and disclosure. Micro security also invnlves protecting an organization's systems, applications and data frnm microcomputer failure, error, omissions and malicious acts by users.

Government organizations placed high priority on contingency planning and disaster recovery, which was also ranked as one of the top three security priorities in last year's survey.

Hnwever, contingency planning is no longer merely a governmental concern; nongovernment nrganizations are also beginning tn recognize the importance of formal planning for business continuity.

Most respondents said service continuity is almost as important to their organizations as data integrity and more important than confidentiality. Because directives from the Office of Management and Budget require government organizations to implement contingency planning and data recovery schemes, the government results were expected. It is noteworthy however, that business and industry placed so much emphasis on contingency planning.

When it comes to implementing contigency measures, most organizations consider the issue to fall under DP's domain. In addition, many companies tend to put off contingency planning until tomorrow.

According to Ernst & Whinney, contingency planning is a business issue, not a data processing issue. It is an issue that organizations must address today, before service interruptions affect business in terms of lost time, business opportunities and revenue. As everyone relies more on complex systems and networks, contingency planning programs must ensure that organizations can continue daily operations without these systems.

The survey also asked about the effect that NSDD 145 is having on security activities in the public sector. NSDD 145 is apparently not meeting its intended objective of actively involving the National Security Agency and the National Computer Security Center in advising industry in security matters.

Only 6% of the nongovernment organizations said the directive has significantly affected their security activities, while 46% said NSDD 145 has not affected their organizations in any way. Also, even though government organizations are required to observe the directive, only 24% of the government respondents reported a significant impact on their organizations because of NSDD 145.

Ernst & Whinney findings indicate the rate at which industry accepts and implements information security and contingency plans depends heavily on the emergence of new standards for due care in security. These standards must be based on security policies that are more relevant to industry than those currently advocated by the National Center for Computer Security under NSDD 145. The standards-setting process must be a joint effort between industry and government, possibly under the auspices of an organizatioo such as the Institute of Electrical and Electronics Engineers, Inc. or the American National Standards Institute.

Losses continue to result from security mishaps; 51% of the respondents reported financial losses within their companies because of security problems. Government and nongovernment organizations showed similar responses. Consistent with last year's results, most respondents reported minor losses (less than $10,000 during the past two years) or no losses. However, 12% of the respondents reported losses of $50,000 to $500,000 during the past two years.

Financial losses are not the only losses at stake, however. Thirty-two percent of the firms surveyed reported nonfinancial losses. Unauthorized access to data by employees was reported as the leading cause of nonfinancial loss. Of the 24 respondents who cited unauthorized access as the leading nonfinancial security event, 19 cited employees as the perpetrators; only 5 respondents listed hackers as a concern. Survey results indicate that hackers are generally perceived to be an embarrassment or nuisance to security but not a serious threat.

Organizations are concerned about protecting both computer and noncomputer data. In a comparison of government and nongovernment organizations, 60% of tbe government organizations focused on protecting both types of information, but only 40% of the nongovernment organizations cited both.

Classified vs. public data

Whetber protecting computer or noncomputer data, respondents indicated that their organizations handle various types of information ranging from public to government classified. The distribution of this information varies significantly between government and nongovernment organizations. While 31% of government organizations primarily handle "government-classified" data, only 4% of the nongovernment organizations handle government-classified data. Fifty-two percent of the data handled by nongovernment organizations is "company confidential or proprietary" information, but this type of data accounts for only 23% of the data handled by government organizations.

Computers have become an integral part of our society. In fact, they have become so important that when something interferes with their effective and intended use, segments of society may become handicapped.

Management is focusing on the need to provide for integrity and confidentiality of the information it uses to plan, control and provide products and services. Management also understands its responsibility to plan for the continuity of its services.

Once management recognizes the need for effective security, it must come up with proper solutions to ensure that organizations can maintain the confidentiality, integrity and continuity of their information systems services. ◆

Survey respondent profile

Ernst & Whinney gathered information for its 1987 Computer Security Survey at the Computer Security Institute's annual conference in Atlanta in November 1986. Approximately 1,000 three-page questionnaires were distributed at the conference with 562 returns.

Survey respondents represented 11 industry groups, with two-thirds coming from government (25%), manufacturing (18%), financial services (15%) and insurance (9%).

Most of the responding organizations are large and have large DP departments. Forty-seven percent have more than 600 employees in their DP departments. Twenty-one percent came from organizations with 201 to 600 DP employees; 21% have a staff of 51 to 200 employees; and 11% have less than 50 DP employees.

Fifty-eight percent of the respondents were actually employed in the security management functions of their organizations. These included information security managers (30%), security officers (14%) and security specialists (14%). The remainder of the respondents came from computer and DP functions, accounting positions and various management positions. — TONI B. FISH

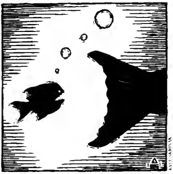
EMPLOYEE CRIME

Insider crimes threaten corporate well-being

BY MARTIN NABUT

The whole notion of computer security has a quality of intrigue. It conjures up ideas of industrial espionage, no-holds-barred competition, laptop-toting terrorists and other felons playing fast and loose with sensitive information belonging to banks, corporations and government agencies.

But many executives say those ideas are more suited to spy novels than to reality. The fact is that despite the increase in personal computer-to-mainframe links, in spite of local-area networks (LAN) growing chaotically and opening new entry points to would-be data thieves, data base theft basically is, has been and probably will continue to be primarily an insider's crime.



MIS directors, security managers and industry consultants agree that the breaking and entering aspect of data theft, though widely reported, is less the game of clever hackers than of disgruntled employees. As an MIS director at Morgan Stanley, Inc. in New York puts it, "It's easier to corrupt a human than a security system."

That executive, who asked not to be named, and others at major corporations, say that both hardware and software technological solutions are useful in preventing an outsider from getting into a data base, but an unhappy employee with access is the real problem.

For example, Hal Jackson, director of computing technology at AT&T Bell Laboratories, compares electronic data theft with the theft of confidential papers from a desk — both are easily accomplished by a dishonest employee wandering company corridors. "Security depends on the integrity of people," Jackson says.

Unfortunately, there are no hard numbers on data thefts or on other electronic crimes because records are kept only for crimes that are prosecuted. While cases involving flamboyant outside hackers are widely reported, many inside thieves caught compromising a company's system are quietly dismissed from their jobs without fanfare or legal action.

Why the corporate reluctance to publicize or prosecute? Jay BloomBecker, director of the National Center for Computer Crime Data in Los Angeles, says that employers often shy away from prosecution because they view it as an admission that their security system can be breached. Publicity in such cases could cause significant loss of business. BloomBecker also sees this trend as "perhaps a basic cynicism that the criminal justice system really works in cases of electronic crime."

Thus, although 47 states now have laws against computer theft, only 75 cases have been prosecuted in the last eight years, and more than 80% of those prosecuted were insider jobs, according to the center's statistics. BloomBecker claims the most common job classifications of data thieves are programmers, computer input clerks, bank tellers, insider-outsider combos and students. The latter group includes teenage hackers as well as college pranksters.

The ambiguity of computer crime statistics is also in evidence when trying to identify the victims of such misconduct. According to the National Center for Computer Crime Data, the most sinned-against faction is the commercial user, a group that includes nearly everyone. The No. 2 and No. 3 victims in this list are banks and telecommunications companies, respectively.

Banks are inevitable victims because,

Nabut is a free-lance writer working in Morristown, N.J. Now retired, he previously was employed by AT&T for 20 years as a public relations specialist to quote Willie Sutton, the infamous bank robber, "That's where the money is." The data that bankers need may be spread over scores of computers in an international network.

Every morning hundreds of bank customers, mostly corporate treasurers, dial up their banks' central data bases to check their companies' cash flow and to authorize the transfer of funds between accounts. Each day, these systems handle instructions governing the flow of billions of dollars.

> **"It's easier to corrupt a human than a security system."**
>
> MIS DIRECTOR
> MORGAN STANLEY INC

Allowing so many people to have access to a bank's system increases the risk of a security breach, of course, but it saves the banks millions annually ay reducing manpower requirements and saving time.

The question is, Can user-friendly reach a point at which it makes a system abuser-friendly?

Banks are not the only organizations wrestling with the conflict between security and the free exchange of information. Bell Laboratories, for example, has long been an advocate of the free exchange of information. However, according to Jackson, "Free exchange of information is sometimes at cross-purposes with security considerations, so we have to come up with reasonable compromises. [We're] often confronted with having to make a trade-off between security and efficiency for system users.

Integrity at stake

"There really aren't any remedies for disgruntled employees compromising security," Jackson says. "It comes down to the integrity of people."

In Bell Labs's case, security education begins at home. Jackson's division combines the MIS functions of technology and security to manage a corporatewide program that involves employees in activities such as watching videotapes to raise employee consciousness about safeguards, a security board game and cartoon-titling contests.

Although the threat of insider data theft is a grave concern, AT&T, for one, sees opportunity in the situation. A consultant version of an internal AT&T program is now on the market and, according to the firm, has had a very encouraging response from both large and small companies.

The program can range from full-blown consultation, including diagnosis of a firm's security needs and development of tools, to labels for floppy disks to seminars for staff members. A 20-minute employee training videotape called "It's Your Move" is part of the program or can be bought separately from AT&T fur $195.

The tape features James Olson, AT&T's chairman, stressing the need for computer security. As an alternative, users can edit Olson out and put in their own chief executive officer.

Mary Tiffany, AT&T marketing manager for the program, admits, "It's not a quick fix. You can't vaccinate your employees with some security-awareness serum and expect a cure."

Don't forget outsiders

Because computer crime statistics list telecommunications as the second most victimized industry, it is not surprising that AT&T is involved in a security-awareness program. Companies such as AT&T must not only concentrate on insider theft but must also remain vigilant concerning outsider misconduct.

In general, telecommunications organizations are vigorous in prosecuting data thieves. These companies should be; telephone links are the common entry points for outsiders bent on theft or mischief (simple or malicious). In fact, existing technological fixes are aimed at denying this entry point to the would-be data thief.

The most sensitive spot in the telephone link between a personal computer and a mainframe is the modem. Hackers have found ways of rummaging around in telephone networks, listening for the characteristic signal indicating a modem, then, by trial-and-error deduction, finding the number of digits need to access the line.

This modus operandi was witnessed in the well-publicized 414 Gang incident, which occurred a few years ago and involved a group of Milwaukee teenage hackers, living in the 414 area code, who gained entry to mainframes at the Los Alamos National Laboratory in Los Alamos, N.M., and access to New York-based Memorial Sloan-Kettering Cancer Research Institute. They accessed these sites using a GTE Telenet Cnmmunications Corp. Telenet network.

Thwarting such incidents

To thwart this type of crime, Mitel Corp., a telecommunications OEM, is now marketing a callback system, the Security Access Controller, that masks a modem so that a backer poking around in a network does not know he is on a data line. A PC user reaching a modem enters his password and the Security Access Controller cuts the connection and calls him back un an authorized line. Mitel offers three levels of security, each putting more intricate authorization requirements on data base access.

How secure is the callback system?

Mitel's director of telecommunications planning, Bill Kirkpatrick, says there is a method for defeating any callback system. However, a criminal using tricks would require in-depth knowledge of central office operations and bad better be prepared to spend weekends on the road.

According to Kirkpatrick, to overcome the callback system, one must know several discrete pieces of information about central office operations and know how tu apply them in a particular order.

> **"You can't vaccinate your employees with some security awareness serum and expect a cure."**
>
> MARY TIFFANY
> AT&T

The thief would also need access to central office test equipment.

An obstacle still remains: The culprit cannot gain access from one spot; he would have to travel to both ends of the connection

Kirkpatrick explains: "Hackers are computer oriented; they just don't know enough about central office systems."

Apparently subscribing to the notion that it takes a hacker to beat a hacker, Mitel employs what Kirkpatrick describes as "industrial hackers" — a group of highly skilled computer technicians, with a full bag of tricks, whose job it is to try to crack the system.

So far, no one has breached Mitel's system, according to Kirkpatrick.

In addition to the use of the Security Access Controller on its own network, Mitel stresses security awareness to its employees and customers. This emphasis includes frequent changes of passwords and encouraging complex passwords that hackers cannot easily guess.

AT&T's Datakit offers another kind of technological fix. Datakit has features that let MIS restrict mainframe access to a limited number of nodes on a network.

Another technological answer to insider and outsider security breaches is encryption. Starting in 1988, an encryption method invented by the National Bureau of Standards will be mandatory for banks dealing with the U.S. Department of the Treasury. Dennis Branstad, one of the encryption method's inventors, says the system guarantees that a message has not been tampered with and that only the rightful recipient receives it.

Determined data thieves

However, a former official of Bankers Trust Co. in New York says that government regulation, rather than confidence in the efficiency of encryption, is the motivation fur using the new encryption method. "A determined data thief can always find those points in a computer net in which the data is in clear text, without encryption," according to the official.

Are there, then, technological solutions that guarantee perfect security? Possibly, but they won't come easy or cheap, according to Les Earnest, associate chairman of computer science at Stanford University in Stanford, Calif. In addition, developments in computer systems give birth to new classes of problems.

Earnest points to LANs as an example. Stanford has 60 interconnected Ethernet LANs for its campus system so that "any workstation can listen to a lot of people on the net." While the network's size and connectivity are impressive, there are drawbacks to a large net. As the network grows, there are more and more opportunities for hackers to gain access to unauthorized data bases in the system.

In fact, gaining what others might call unauthorized entry to the net seems to be an academic challenge for students and accepted by the faculty. Earnest explains that there are break-ins to the Stanford system almost daily, "but it doesn't enormously upset us," he says, unless there is malice involved. If someone attempted to destroy data, Earnest says, "we would go after him."

War Games to the rescue

BloomBecker of the National Center for Computer Crime Data sees a kind of oddly positive force in hacker publicity. He says the movie *War Games* and the arrest of the 414 Gang were probably the major forces leading to the computer crime laws now in effect in all but two states.

"Computer security professionals have been trying to get the public's attention for two decades, but it seems to have taken the kids to drive the message home," BloomBecker says.

However, despite the state legislation and the Computer Privacy Act recently passed by congress, BloomBecker says that computer crime is increasing and becoming more expensive.

The cost of crime

Malicious tampering with computer systems and data costs the owners of these systems an average of $93,600 per incident Thefts of programs or data cost an average of $55,166 each. Outright criminal theft nets the criminal an average of $10,517, according to the National Center on Computer Crime Data.

There are, of course, the rare examples of extravagant crime. Stanley Mark Rifkin, a former consultant, made an illegal electronic transfer of more than $10 million from the Security Pacific Natinnal Bank in Los Angeles to his Swiss bank account. Knowing the bank procedures, Rifkin got past a security guard by flashing an outdated pass and found the day's security code for wire transfers of funds posted on a wall.

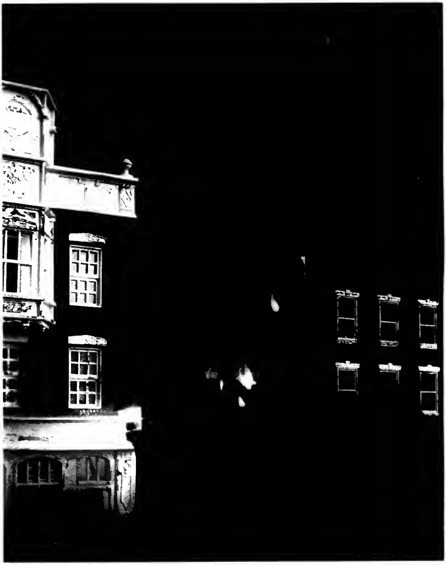
The majority of computer crime, however, is what BloomBecker calls "data diddling," and there are many, everyday variations, including the following:

- A department store sales clerk changes delivery addresses for a shipment of goods, diverting it to accomplices.
- A programmer at a savings and loan company transfers $5,000 into his personal account and makes phony debit and credit entries to cover it up.
- A county district attorney in Colorado tries to delete a pair of speeding tickets from the motor vehicle bureau's computer system.

To fend off both the malicious computer systems hacker and the employee with the chip on his shoulder, the computer industry must foster a kind of computer morality.

In a report by the National Center on Computer Crime Data called "Computer Crime, Computer Security, Computer Ethics," BloomBecker calls for the development of a "mainstream computer ethic" to fight computer crime.

Without additional efforts to shore up computer security and develop computer ethics training, BloomBecker says, "computer crime will continue to be a growth industry." ✧



GEOFF O'CONNELL/PATRICIA GAUDETTE

The disaster business

BY STAN KOLODZIEJ
SENIOR EDITOR

Disaster recovery is a big business as well as big money these days. In fact, International Resource Development, Inc. of Norwalk, Conn., projects a combined U.S. data center/disaster recovery market worth $510 million for this year.

The number of MIS personnel concerned with disaster recovery planning has taken off. In five years, the Delaware Valley Disaster Recovery Information Exchange Group has grown from a regional constituency based in the southern New Jersey/Philadelphia area to a national forum of nearly 600 corporate members.

Former Delaware Valley group members have even undertaken some missionary work, establishing associations in other parts of the country.

On the West Coast, the Association of Contingency Planners is becoming a vocal sounding board for disaster recovery planning. Other associations are getting under way across the U.S., offering telephone numbers to call for answers to disaster questions from MIS. Some new members are proselytized, others come out of curiosity, still others are pointed in the right disaster planning direction by senior management. The fact is, disaster recovery has become a big bandwagon, and a lot of MIS are jumping on.

"The whole focus on disaster recovery has changed," according to Jack Bannon, manager of information security at Cherry Hill, N.J.-based RCA Corp. and president and cofounder of the Delaware Valley Disaster Recovery group. "In the old days, disaster recovery was just a plan drawn up to appease the auditors. Now, it's serious business."

Boston-based Fidelity Investments' disaster recovery plan, page 28

No wonder. The financial fallout in the aftermath of disasters is grave indeed. Companies dealing in disaster planning are quick to dole out a litany of statistics that point to the dire consequences of not planning for disaster.

One disaster planning firm, for instance, pegged the cost of an "unscheduled" interruption of central DP services for a typical large insurance company at $275,000 a day and for a typical major airline at a catastrophic $20,000 a minute.

Wayne, Pa.-based Sunguard Recovery Services, Inc., a major player in the disaster recovery market, claims that a large bank would be out of business in one or possibly two days without the use of a DP center. A distribution company would last just more than three days; a large manufacturer perhaps five days; and an insurance company could linger as long as six days.

The statistics all carry the same message: Computer disaster equals financial chaos. If the message is a scare tactic, then a lot of firms are watching their steps.

The statistics all carry the same message: Computer disaster equals financial chaos. If the message is a scare tactic, then a lot of firms are watching their steps.

"What galvanized us toward recovery planning was a fire in a hotel beside our data center," explains Connie Brock, a vice-president and data security officer at Norwest Technical Services, Inc., headquartered in Minneapolis. "It didn't do any real damage, but it made us see how vulnerable we were."

Robert Lucey, president of Putnam Investors Services, Inc., a Boston-based broker of mutual funds and a company that suffered through a fire last December, explains that although the company's disaster recovery hot site plan worked well, Putnam Investors is still contracting to add extra communications lines and update its entire system of backup procedures.

"We've added a backup generator and battery packs," Lucey explains. "We're taking a hard look at all procedures, making sure we're current. There wasn't extensive damage done to the building, but we still lost power for a week. That frightened us."

Some companies simply have too much responsibility to their clients to ignore disaster planning.

New York's Depository Trust Co., for example, has more than $2 trillion worth of securities in its vaults, probably making it the world's largest custodian of corporate stocks and municipal bonds.

Depository Trust is a cooperative venture of 600 securities firms and has, for all intents and purposes, done away with paper trading, instead giving its members a computerized book entry system. The actual security documents remain in Depository Trust's vaults. Understandably, the company's data security and backup plans read like the security measures for Fort Knox.

Ironically, given their air of conservatism, banks and other financial institutions have become sort of shock troops in disaster recovery planning. In a large way, however, their leading-edge role has been mandated by the government, which has legislated rules directing all national banks and savings and loan institutions to put disaster recovery plans in place.

The wheels of this mandate were put in motion a decade ago when the government issued its Foreign Corrupt Practices Act (FCPA), a rather misleadingly named piece of legislation that enjoins all U.S. companies to establish accounting controls as a legal necessity. Part of this thrust in corporate accountability was the required protection of corporate assets, which, during the years, have been increasingly channeled into computer data bases.

"The FCPA provided the first framework for data center disaster recovery plans," explains Dianne C. Smith, president of the Long Beach, Calif.-based Association of Contingency Planners. "Anyone that has any government contracts, is mandated or regulated in any way or handles securities has to have a disaster recovery plan in place. And that just about includes everybody now."

As the disaster recovery business matures, so do the options. Hot sites have a computer and space available for an organization. Cold sites only reserve a space, or shell; if disaster strikes, a company has to provide its own hardware. Mobile data centers bring everything to firms.

Stationary hot sites can cost hundreds of thousands of dollars

Fidelity invests in leased hot site

BY MARY LOU JORDAN
SPECIAL TO CW FOCUS

When it comes to planning for emergencies, Fidelity Investments takes no chances.

The company's Boston headquarters houses most of its computers. The building's computer rooms have an array of weapons to combat disaster: Halon fire-retarding systems, water detectors under the floors, access controls at every internal as well as external door and enough power from generators to run the computers indefinitely in the event of a power failure.

"Part of disaster recovery is planning to avoid disasters in the first place," explains Liz Foote, director of systems management for Fidelity, the country's second-largest purveyor of mutual funds.

If anything does go wrong, though, Fidelity is ready. The managers and staff would pick their tapes up from the previous night's backup, which is stored off-site, and fly to a leased hot site in Philadelphia.

Since June 1983, Fidelity has contracted with Sunguard Recovery Services, Inc., a Wayne, Pa., firm that provides hot sites and disaster recovery consulting services. "We'd go into the Sunguard facility and restore the operating system and some necessary software. Then we'd start restoring applications that are data specific to a particular business entity," Foote says. Critical operations, like Fidelity's discount brokerage and mutual funds services, would be booted up first, followed by less time-dependent financial programs and internal services.

Fidelity is an IBM mainframe shop that has two 3090 Model 400s and two 3090 Model 200s running all the time. The facilities at Sunguard match headquarters's closely enough to make Fidelity comfortable with its alternate site. "There are some things we can't process at Sunguard because the site is not as big as we are, but there are also things we wouldn't have to process if we were in disaster recovery mode [such as] lots of reports. We'd shed those noncritical operations," Foote says.

Since 1983, Fidelity's MIS department has conducted on-site testing at Sunguard. Four weekends a year, representatives from each department in MIS, making up a group of 10 to 30 people, go to Philadelphia and restore operations from backup tapes. Aided by colleagues in Fidelity's Dallas, Salt Lake City and Boston offices, MIS begins processing transactions dialed in from offices around the country, simulating as closely as possible a normal business day.

It is up to the team at the hot site to make this activity as transparent as possible to dial-in users. Confirmation of success comes in the form of overnight report processing, which tracks all the transactions made that day and checks that they were all handled accurately and completely. According to Foote, "It's basically just like running a mini-Fidelity in Philadelphia for a couple of days," except that all the computers, disks, tape drives, modems, phone lines and terminals are rented and may be used by a completely different firm the next day.

Testing has grown more and more complex during the years as a greater percentage of the firm's normal applications are brought on-line during the false emergency.

It probably didn't hurt the plan's credibility that in March 1983, the same month Foote presented the plan to senior management, Fidelity had a long blackout and then a fire next to the computer room. Her plan was approved, and the first test at Sunguard took place in June of that year.

Fidelity looks at expenses for recovery planning as an investment for the future.

As Foote explains: "In a company like Fidelity, which has its soul tied to DP, a large amount of the money we make in a day depends on DP. We immediately start losing revenue if that support is not available."

The advantages of a rented hot site over a reciprocal agreement or casual plan include compatible equipment, the availability of equipment any time it is needed and, most importantly, the ability to test the system before it is needed, Foote says. And what are the advantages for Fidelity of a rented hot site like Sunguard's over maintaining its own permanent site? "The cost of maintaining a site exclusively for our own use is astronomical," she maintains.

In the future, Fidelity plans to build up its Dallas facility to the point at which it can handle many of the critical disaster operations now planned for Sunguard. When the Dallas facility is ready to handle critical operations, the less crucial operations will be moved to Sunguard during a disaster.

Fidelity has no plans to give up its rented hot site. Until Fidelity has "multiple computer centers with excess capacity, which won't happen any time soon," Foote says, she's going to stick with a good thing.

Jordan is a free-lance writer and technical editor who lives in the Boston area.

to reserve each year, though the average cost is less than $200,000. That price is still enough to stop all but the largest corporations with the biggest computer arsenals from keeping both space and machines on perpetual hold.

It's expensive insurance, but the benefit is peace of mind. Should calamity come calling, a corporation can gather critical staff and tapes and beat it to a waiting computer facility where the company's DP facilities can be up and running again in a matter of hours.

This situation, in fact, is exactly what occurred in Montreal last October when a fire ripped though the headquarters of Steinberg, Inc., a Canadian retailer (see story page 30).

Though the fire happened in the early hours on a weekend, key Steinberg MIS personnel were quickly rounded up and flown to a waiting Comdisco Disaster Recovery Services, Inc. hot site facility in Carlstadt, N.J., while the company's important financial tapes were trucked across the border.

In hours, Steinberg had its important applications up and running, and it was business as usual. This example is as pure a drama and good endorsement for the efficacy of disaster recovery planning as any screen writer could conceive.

> **If a company does not have adequate communications planning, it does not have adequate disaster recovery.**
>
> OIANNE C. SMITH
> ASSOCIATION OF CONTINGENCY PLANNERS

The fact that the Steinberg case involved a billion-dollar company, extensive damage and the commodity of plenty of press attention (Steinberg, in fact, has been unusually open with the media about the disaster and its aftermath) has made the incident a cause celebre with disaster recovery firms. For years, the industry could only point to minor incidents or reams of impersonal statistics. Now they had the smoking gun.

Cold sites, or shells, are not as costly as hot sites, but a major drawback is the possible unavailability of equipment when it is desperately needed. Even the closest and most secure of client-vendor relationships will probably not get computers delivered within 24 hours of a crisis. The average lag is usually 24 to 48 hours or more.

"For too many businesses even that short a time would be a nightmare," says Rick Effgen, president of Chi/Cor Information Management, Inc., a consulting firm in Chicago.

Five years ago, this time lag might not have been too long. These days, however, nearly all critical applications are real-time and on-line; batch processing has been on a downslide for a decade. Where batch is still used is primarily in applications not immediately critical to companies.

A number of companies have even assembled moveable hot sites and taken them on the road. These mobile trailer units can motor to a disaster site, set up shop in the corporate parking lot, plug into existing communications lines and offer a kind of itinerant processing.

As part of its Compuguard disaster recovery service, for example, Compusource's Provident Recovery Systems mobile unit is composed of several trailers that can be strung together like a Lego set to form 2,000 square feet of computer space housing a full IBM 4300 system and a complement of peripherals.

Cary, N.C.-based Compusource claims the mobile units can be set up at a disaster site in a few days.

"The ability to relocate back to the customer's original site, the assured access to a mainframe configuration and the use of a customer's existing telecommunications network are the real benefits [of this service], according to Compusource President Wayne Edge.

Today everything is linked. Communications backup has now become a major component in disaster recovery planning.

"Divestiture has thrown the onus of telecommunications back onto client companies," says Ron Bosco, president of Federal Engineering, Inc., located in Fairfax, Va

"Until 1984 telecommunications in the U S. operated in a cloud. Customers didn t have to know about communications because a carrier handled it. Divestiture blew the lid off that."

No coffee, plenty of POS

Smith says, simply, that if a company does not have adequate communications planning, it does not have adequate disaster recovery. 'During a major electrical storm a few years ago I happened to be in a Denny's coffee shop that lost power," Smith says. "It couldn't heat the coffee, but its point-of-sale [POS] system was up, and that impressed me. It had installed an independent network for its POS

' This situation doesn't mean that your mainframe site has to be directly linked to a hot site, ' Smith explains "It just means you have to do some alternate planning. You have to develop the kinds of networks that are multinodal, in which no matter which node you lose you can still operate "

That idea makes sense to Don Moeller, disaster recovery manager for Comvac Disaster Recovery, Inc , of Independence, Ohio Comvac's new cold shell facility is equipped with 200 pairs of dial-up

Fire tests Canadian firm's disaster plan

BY KRISTEN NOAKES-FRY
SPECIAL TO CW FOCUS

On Oct 26 1986, a fire destroyed the central data center of Montreal-based Steinberg, Inc , a $4.5 billion Canadian retailer that operates a chain of hundreds of supermarkets, restaurants and stores and employs 30,000 people The resulting water damage and power and communications outage put Steinberg's data center out of business and halted DP services to the entire Steinberg chain.

Within two days, Steinberg staff members working at Comdisco Disaster Recovery Services, Inc 's New York Metro Recovery Center, located in Carlstadt, N.J., restored DP activities to the entire chain and was soon able to issue a payroll to thousands of employees.

The following is the chronology of events'

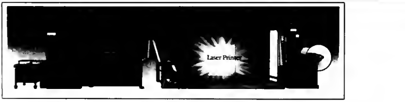
- **Oct. 26.** Fire is discovered at 6:00 p.m.
- **Oct. 27**. The disaster is reported to Comdisco at 11:45 a m Steinberg's 25-member disaster recovery team leaves from Montreal to join the Comdisco recovery staff and technicians at the hot site in Carlstadt. Ten thousand tapes from the Steinberg data center are loaded onto a 45-ft trailer, put through customs and rushed to the Carlstadt site. Seventy members of Steinberg's DP management and staff relocate to a cold site in Montreal.
- **Oct. 28.** Critical systems are restored to stores
- **Oct. 29.** Normal business is resumed. Weekly paychecks are distributed to 28,000 Canadian employees

The key to Steinberg's survival was its prior preparation and planning At the time of the fire, Steinberg was one of a consortium of Canadian companies instrumental in developing a cold site at Comdisco's Montreal Recovery Center. The firm was also a hot site subscriber at the New York Metro Recovery Center and had a contingency plan in place that had been tested earlier in October when employees practiced a move to the Carlstadt center.

The following tips may help companies stay in business after a disaster strikes:

- A firm needs management commitment.
- A firm needs a detailed disaster recovery or contingency plan in which everyone in the company is involved.
- A firm needs disaster training for employees
- A firm needs to rehearse and update the plan.

Noakes Fry is an associate editor and analyst for *Datapro Reports on Information Security* published by Delran N J based Datapro Research Corp This article appeared in the Datapro report



or multipoint lines and is aimed at servicing medium-size customers that are more apt to center their computing on minis than on the bigger mainframes.

It also makes sense to Nathan Braught, consultant with Oak Park, Ill.-based Ecos Environmental Systems.

"You have to remember that a lot of the power technology driving today's computers is 40 or 50 years old," Braught says. "It's getting worse every day."

Other options are appearing. Now a very competitive market, the disaster recovery area used to be almost exclusively an IBM domain where big players like Comdisco Disaster Recovery Services and Sunguard catered to heavyweight IBM mainframe custnmers. Now, some disaster recovery firms are bucking the trend and offering more regionalized services to smaller groups of clients using computers from Prime Computer, Inc., Data General Corp. and other non-IBM vendors.

O'Neill Data Systems of Lenni, Pa , for example, provides DG computer users with backup and recovery services, while Dallas-based Transfirst Corp. has gone into business with Comdisco to offer disaster recovery services to Tandem Computers, Inc. customers.

"I think we're seeing a stronger secondary hot site market emerging that does not try to be all things to all people," Chi/Cor Information's Effgen says. "This market's main attraction is going to be price, and [its players] are going to try and position themselves away from the big guys."

Among the least expensive of disaster recovery options is to contract a reciprocal agreement with another firm to provide for processing on its system.

> **The one big weakness in most reciprocal agreements is the possibility that a company can ill afford to give another firm processing time when it is needed.**

But the computer industry keeps changing. The feasibility of arranging reciprocal agreements is not so obvious now. RCA's Bannon points out one big weakness in most reciprocal agreements: the possibility that the other company could ill afford to give another firm processing time when it is needed.

Installing dual, or mirror, data centers is probably the most reliable disaster recovery option. It is also the most costly. One drawback lies in maintaining dual data center applications that employ redundant equipment.

"When we originally implemented dual data centers in the 1970s, there weren't very many good hot site services available," Norwest Technical's Brock explains. "In those days, most transactions were batch, not on-line. During the years, however, it became increasingly inconvenient to have work divided between data centers. At the same time, hot site services were improving."

Charles Perkins, a supervising consultant with the management consulting services division of Coopers & Lybrand in Baltimore, claims that most dual data center applications employ redundant equipment and can waste money.

"There's overkill with many of the larger dual data sites," he says. "It gets very expensive."

Whatever option an organizations chooses, everyone seems to agree that one of the first steps in disaster recovery planning should be the identification of critical applications. Should problems occur, these would be the first a firm would bring up.

"But even that's not as obvious now," Federal Engineering's Bosco explains. 'The greater use of computers in business is changing security game plans. It used to be payroll accounts receivable and other financial considerations that were always identified as the major applications tn go up first. That's

not necessarily true today.

'For example, I have a manufacturing client and asked it what was critical to its business. Almost by rote it answered, 'Payroll.' We replied that come payroll day, if the system was still down, the company could bring in blank checks, have temporary help fill them out and have them signed by the president. That wasn't critical. What was critical was its shop floor control, which was run by computers. If that went down, the firm couldn't produce to meet demand in order to survive. The company wasn't aware of just how critical computers had become to every part of its business," Bosco says.

Putnam's Lucey points out that his bank was more than clear on pinpointing what had to go up after disaster struck.

"We have two critical applications," Lucey explains. "One is shareholder accounting for the people who give us their money to invest. The other application is the reverse side. Once we have the money, we have fund managers who buy and sell various securities in the open market. We have to keep track of those transactions as well so we know what the value of the mutual funds are at any point in time.

> **"People are realizing that it is not much good if you can get into the data center but the user areas are gone."**
>
> RICK EFFGEN
> CHI/COR

"Both of these [applications] are crucial to our survival. And the only way to make sure they are secure is to keep testing," Lucey says.

Catherine Weyhausen is corporate security manager at AT&T in Cherry Hill and one of the people behind AT&T's "It's Your Move" internal computer security program. She explains that part of the program requires AT&T department managers to periodically match their critical applications against a policy guide issued by the company.

"The 'It's Your Move' program is a series of checks and balances down the [managerial] line," Weyhausen explains. "Identifying important applications is a major concern."

However, Effgen advises against always weighing everything in relation to the computer when working on contingency plans. "The data center is usually the place where security tends to start," he admits. "But in the Norwest [fire in 1982], the Steinberg and the Putnam disasters, the data centers were fundamentally unharmed; they were just inaccessible. And people are realizing that it is not much good if you can get into the data center but the user areas are gone. There are certain things that will certainly be dependent on computers and other things that will not be so dependent.

"The largest single issue that clients avoid upfront," Effgen adds, "is what I call postdevelopment issues involving plan maintenance, ongoing testing and moving the [disaster recovery] program into user areas. You have to maintain a plan and constantly test it."

Effgen agrees that critical applications are changing as businesses change. "Today, people who are smart do what is called risk analysis," he says. "We go in and interview what are perceived to be the critical departments. We'll interview users and see what's going on and get a sense of what the impact would be of losing an application from a legal, operations and financial standpoint," he says.

Smith from the Association of Contingency Planners says that "we tell everyone not to plan for a specific event. That's not the one that will happen."

Lived to tell about it

Those who have been through disaster might concur.

The communications managers at Pacific Bell in Riverside, Calif., who recently spent time cleaning up the mess to their switching system caused by blasts from a disgruntled former employee's shotgun, would probably agree.

So would Sheldon Harris, vice-president of data processing and information services at Bankers Life & Casualty Co. The Chicago company, which has an extensive disaster recovery plan in place, spent a frustrating time last year trying to arrive at the source of a problem that kept crashing the tape drives of their IBM mainframe. For no apparent reason, Harris explains, the mainframe would periodically stop to conduct communications/interface checks. The situation was causing havoc with the firm's on-line applications.

Harris says he brought in everybody, the bank's MIS people, people from the tape drive manufacturer and consultants. Nobody could figure it out. Finally, Harris brought in some people from Ecos Environmental Solutions. Ecos did some detective work and came up with an answer.

"They checked the power system, everything," Harris explains. "Finally, Ecos correlated the factor of low humidity and the high incidence of interface control checks. It seemed that carts and workers in the computer room were building up a large amount of static electricity that was not dissipating. As soon as a cart or one of the employees touched the mainframe, it would zap the drives.

"I admit it's embarrassing," Harris says. "It took us six months to figure out. And all the time it was right under our noses." ❖

Site uptime management

An ounce of disaster prevention is worth a pound of cure

BY KENNETH BRILL

In addition to planning for disaster recovery, MIS must eliminate or minimize the potential for disaster in the first place. By maintaining a state of preparedness for both people and systems, MIS can help its organization skirt a catastrophe.

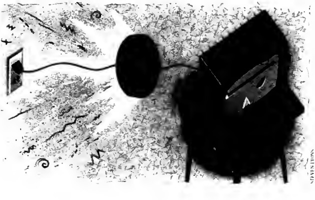
The capacity for avoiding disaster is the result of a carefully thought-out management process called "site uptime management." In a new facility, site uptime management begins with a critical yet deceptively simple conceptual engineering block diagram that lays out equipment choices and capacities, bypassing interconnections, redundancies, maintenance procedures and off-line testing as well as human factors.

This diagram determines the disaster risks the site should be capable of withstanding. It also sets a maximum limit on uptime reliability.

Site uptime management continues as construction proceeds and the site takes physical shape. MIS runs acceptance tests knowing that bugs exist and that it must wring them out before the site goes on-line. The staff needs to be trained and rehearsed on what to do in the event of an emergency.

Even then, the job isn't over. Site uptime management is a continuous process of manufacturing uptime and controlling downtime risks through preventive maintenance and testing. This process will last indefinitely or until the site is taken out of service.

Although disaster avoidance is at the heart of site uptime management, an annual disaster risk inspection may be appropriate. Similar in concept to the fire and accident hazard inspections made in very large plants by insurance carriers, the purpose of the risk inspection is to assure all involved that the company is following the site management plan, that it is competently performing scheduled preventive maintenance, that site equipment is in good repair and that there are no obvious disaster hazards



STEVEN LYONS

The definition of a physical disaster has been subtly changing as uptime expectations have increased. Only five years ago, relatively few MIS departments were trying to achieve uptimes higher than 95%. Today, this situation has almost totally changed. With the advent of on-line transaction processing, uptime expectations have grown, and levels of 98% and even 99.5% are now not all that uncommon.

In recognition of the growing importance of on-line systems, the traditional concept of a catastrophic disaster needs to be expanded to include "site downtime." From an end user's standpoint, it doesn't matter whether the computer is down because of a fire or a momentary power flicker; the results are the same: The user can't perform his job. In large organizations, this event quickly becomes a customer service, sales or accounting disaster with large dollar implications.

Brill is a site uptime consultant and president of Computersite Engineering, a Cambridge, Mass.-based engineering consulting firm specializing in site conceptual design, acceptance testing and management of uptime.

A site usually has up to 17 environmental subsystems. These subsystems must be working as a life-support network before computer hardware can be powered on. These subsystems form an interconnected and interdependent network so that overall site reliability is determined by the weakest subsystem link. As a result, the failure of an insignificant $5 part can result in unexpected and potentially expensive site downtime.

The site subsystems are as follows:

- **Uninterruptible power systems**: Including utility service entry, high-voltage transformers and building switch gear; lightning protection, electrical power risers and distribution, 60Hz uninterruptible power supply (UPS); UPS air-conditioning, 415Hz frequency converter or UPS; battery plant for UPS; emergency generator, computer room power distribution, grounding.
- **Cooling systems**: Including mainframe process cooling, computer room air-conditioning and humidity control.
- **Human factors**: Including training, testing and rehearsing staff.
- **Other critical systems**: Including detection and suppression; raised flooring and environmental surfaces, physical security and access control; monitors, alarms and remote operating.

While site malfunctions are usually rare, when they happen, they have a profound impact on everyone involved. Because site malfunctions typically tend to run in cycles with a second and third malfunction usually taking place before the original problem is found, computer operations can just be returning to normal when disaster strikes again. A single cycle of site malfunctions can easily put overall computer uptime goals out of reach for an entire quarter or even for the entire year in especially serious cases.

When a site crashes, everything dependent on the site must also crash, with damage to both hardware and software a virtual certainty.

If computer hardware won't restart once the site is back up, MIS must identify the defective components and then either repair, replace or bypass them. Only after hardware uptime has been restored can the task of assessing software damage begin.

The length of time to recover software and data will depend on what the machine was processing at the time of the site malfunction and how far back operators must go to find a checkpoint from which to start reprocessing.

Assume that a site malfunction occurs. Depending on the size and complexity of the site, it might take between 15 minutes to one hour for someone to diagnose what went wrong, fix it and decide that it is now safe to try bringing computer hardware back up.

Again, depending on size and complexity of the site, it could take 30 minutes to one hour to restart hardware and an additional 45 minutes to two hours to restore software. Thus, a momentary site malfunction lasting only seconds could be amplified into between one and one-half hours and four hours of computer outage, which, for large on-line systems, could represent a cost of many tens of thousands of dollars.

For 99% uptime, the total duration of computer outages cannot exceed three and one-half hours per month based on a prime time of 13 and one-half hours of operation six days a week. A single momentary power flicker invisible to the eye can easily consume this and more, leaving no reserve for other problems.

> **A momentary site malfunction lasting only seconds could be amplified into between one and one-half hours and four hours of computer outage, which, for large on-line systems, could represent a cost of many tens of thousands of dollars.**

MIS must systematically identify potential site disaster risks individually for each of the 17 subsystems and then examine how each interacts with one another as a system. It needs to then rank these risks by both the probability of their occurrence and by the duration of the resulting computer outage while uptime is being restored. With proper site design, preventive maintenance and regular testing, these downtime threats can be greatly reduced or eliminated.

Take, for example, the risk that the emergency generator won't start or fails to carry its load. From a reliability standpoint, about the worst thing that one can do to an emergency generator is exercise its engine with no load. If this is done over an extended period, the carburetor or fuel injectors are likely to get clogged, which can cause the engine to fail when it has to pull an emergency load.

If this generator fails, the consequences are that both the computer room and UPS will lose computer process cooling and air-conditioning. If the generator is not successfully restarted or if utility power doesn't return, it only takes seven to 10 minutes for the ambient computer room temperature to rise from 70 degrees Farenheit to 90 F. At this temperature, controls should automatically remove power from the computer and the UPS, causing a crash but ensuring that neither gets cooked.

The typical reason that generators are not load-tested is that the only load available is the computer itself. Often, the maintenance people want to test the generator (or any other piece of similar equipment) for emergency readiness. However, the only way they can test it is to use the computer as a live load, which the DP people won't permit. As a result, a stalemate develops and the equipment remains untested until an actual emergency occurs. If it fails then, there is usually plenty of finger pointing.

MIS can learn several things from this example. First, testing the generator under load is critical and greatly increases readiness. Second, if the equipment necessitates professional maintenance, a means for testing equipment under load and independent of the computer must be provided in the design and construction of the site. Third, if the generator fails to start, within five minutes someone in authority must decide whether to order a computer system shutdown to avoid the hard crash that will happen when automatic temperature controls take over. Rehearsing key personnel on how to take charge and what to do in an emergency situation can greatly reduce potential downtime damage.

Site uptime begins with a statement of management's goals that include not only uptime but also a time limit on the duration of site downtime before uptime must be restored.

The downtime risks a company must protect against are affected by site location, geography, weather conditions, location of the site relative to the utility's distribution grid, annual temperature extremes and other factors. After considering these factors, a conceptual block equipment diagram of the site can be laid out showing the equipment to install, interconnections, bypassing, off-line testing capability and how much capacity and redundancy will be required.

Implicit in the block diagram are key strategic planning decisions that will determine future reliabilty. It is very important to keep in mind that once the site goes on-line, it probably can never be completely turned off.

A company needs to anticipate failure modes for every site subsystem and key components within each subsystem. Ways of taking components on- and off-line without disruption to the computer must be designed into the site from the very beginning. In addition to anticipating repair problems, the block diagram must also provide for the performance of regular preventive maintenance and periodic load-testing of selected components without exposing the live computer load to risk or disruption.

To make this scenario more tangible, consider the uninterruptible power system. Made up of 10 subsystems, the purpose of an uninterruptible power system is to control the flow and quality of the electrical energy the computer receives. Each of the 10 subsystems serves a specialized purpose. However, they may not all be required depending on management's stated uptime goals.

Many customers that want a uninterruptible power system end up getting an uninterruptible power supply, or UPS, instead. A UPS is only one of 10 subsystems that must be assembled to form a true uninterruptible power system. At a minimum, air-conditioning and batteries are required to make the UPS an uninterruptible power system.

Even with these extra subsystems, reliable uptime is still not assured. The air-conditioning must be redundant or a slipping blower belt will be magnified into a site crash when the UPS overheats. Without batteries fully ready, a static UPS is very limited in what power conditioning it can perform. Any power failure on the input will be passed through to the output.

Ideally, it should be possible to purchase a factory-made uninterruptible power system from a manufacturer that carefully optimizes costs and benefits, takes advantage of previous mistakes and guarantees uptime.

Uptime results not included

With few exceptions, this is not what generally happens. Instead, the uninterruptible power system's subsystems were designed by the manufacturers and consultants who got paid for rendering services or delivering the product but not for achieving contracted uptime results.

Based on plans and specifications, a low-bid contractor will assemble an uninterruptible power system on a site using major components from at least 15 different manufacturers.

This project is usually done under severe time constraints with little or no quality control supervision. Workers may be unfamiliar with the equipment they are installing or may not understand how to make the interface connections between subsystems.

The only way to know that all subsystems will work is to test the site under simulated load conditions. This means bringing in load banks to test the UPS, batteries, emergency generator and cooling systems A technically competent person who represents the owner's uptime interests should supervise the testing. If the site's conceptual and detailed engineering has been executed well, the initial deficiencies found during testing will cluster around installation problems in interfacing interconnecting alarms and controls.

As full load is applied and maintained for at least 24 hours, additional problems, which are generally easy to fix, will start showing up.

Typical problems that occur include such mishaps as a chilled CPU water pump and an emergency generator fuel pump both getting utility power instead of uninterruptible power system power. In the event of a utility power failure, the chilled water pump would stop circulating coolant through the CPU. The CPU would overheat and a subsequent hard crash would occur even though the machine received uninterrupted power from the uninterruptible power system.

In the second example, the generator would run out of fuel about 30 minutes after the utility fails. If found during testing, these problems are minor. Once the site has gone hot however, any malfunction is serious business.

What to look for in an inspection

It is wise to have an annual disaster risk inspection. Such an inspection of the emergency generator would include a visual inspection of the unit and related controls; checking the starting battery for acid and cable connections; checking the engine for oil and water; starting the engine and observing the exhaust smoke; applying full load and listening to how the sound of the engine changes and whether exhaust smoke changes color; observing the voltage and frequency meters for any sign of oscillation; watching the temperature of the engine rise, shutting the engine off and listening to how it stops, and finally, studying the generator maintenance log for any data on problems that might result in a future failure to carry load.

If similar risk inspections are performed on the other site subsystems, everyone, including top management, will know that everything possible has been done to prevent disaster and that the organization is getting full value from its expensive investment in site uptime equipment. ❖

THE INFORMATION TECHNOLOGY LEADERS

Henry F. Nanjo
Director Systems
and Data Processing
City and County of San Francisco
Age: 58
Budget: $30 million
Cross Country Skier

As the City and County of San Francisco has discovered, there's only one sensible way to evaluate and integrate products into one cohesive information system. And that's with a department strongly guided by an experienced, innovative information services professional like Henry Nanjo.

Henry didn't always have a multi-million dollar budget, with responsibility for the acquisition of hundreds of micros every year. In fact, when he started working with San Francisco's computers 31 years ago, Henry didn't even have a DP department. He simply worked in accounting with his state-of-the-art IBM 305.

Over the years, many of the applications Henry developed have helped keep San Francisco among the country's most innovative users of computer technology.

San Francisco made headlines recently with the first computerized fingerprint matching system. With it, prints can now be matched in less than 3 minutes—a far cry from the 4 weeks required to do the job by hand. Already, the system is credited with helping solve some 40 major unsolved crimes.

Today, Henry is in the process of evaluating both existing and potential vendors of minis and micros—and maintaining an approval list of vendors for purchases made throughout the organization. Every computer-related expenditure, whether it falls within Henry's $30 million budget or the City and County's $60 million budget, must bear the name of a vendor appearing on Henry's approval list.

What little spare time Henry finds, he spends with his sons camping, hiking and cross country skiing in areas like Tahoe, Yosemite Park and the Shasta Mountains.

If you'd really like to reach Henry, you'll find him on Monday mornings with his copy of Computerworld—he's been a subscriber since the first issue. He finds Computerworld's perspective meshes closely with the way he does business, covering everything from mainframes to micros, software and state-of-the-art technologies.

Information Services is full of bright individuals with individual visions. Yet they all seem to have one common insight.

Their favorite newspaper.
Computerworld.

Where you can read
the future

Computerworld 375 Cochituate Rd Box 9171
Framingham, MA 01701 9171 (617) 879-0700
A CWCI Publication
An International Data Group Company

SYSTEM TRADE-OFFS

Don't get locked into too much security

BY REBECCA HURST

If a high-speed computer zipping through data transactions is as sexy as a Porsche turbo, then the security it requires has all the attraction of auto insurance. It costs money, and you may or may not ever need it.

With few visible benefits linked to security, most DP and MIS professionals want to implement a sufficient degree of security without providing more than necessary. At the same time, these managers are trying to balance their need for security with cost, education and the end user's need for reasonably simple access to corporate data.

Some companies have clearer security requirements than others. Organizations such as the government and banks need to protect sensitive information and billions of dollars, so they spend hundreds of thousands of dollars on data encryption systems regulated by the National Security Agency.

However, a great majority of organizations do not need top-of-the-line security, according to Daniel Lynch, president of Advanced Computing Environments, a Cupertino, Calif.-based consulting firm. "Some day, when we come to rely on electronic communications and it becomes a fabric of life, we will need [better security]," he speculates. "Right now, we don't because we have not yet entrusted our lives entirely to the electronic transfer of information."

Already, users rely more on electronically stored information as they gain access to data through their personal computers. With increased PC use, managers are also finding a greater need for security. "PCs are an open invitation to breach security," claims Jack Rodgers, director of marketing for the San Francisco-based

Hurst is *Computerworld Focus*'s senior writer software products division of On-Line Business Systems, Inc. With terminals, all the control is centralized at the mainframe, he explains. When processing is distributed between PCs and the central host, some mainframe controls are lost.

For example, Rodgers says, PC users can put alphabetic characters in numeric files. In a terminal-to-host situation, the mainframe software guards against this. Also, corporate computers lose their ability to provide complete file and record locking

"Some products provide record locking," he says, "but they don't protect files." Therefore, users can accidentally wipe out each others' file updates and cause the system to lose its data integrity, Rodgers notes.

The use of PCs at Chicago-based United Airlines has brought a need for additional security, agrees Suann Lively, a staff analyst at the airline. "More and more, our company is using PCs for sensitive data," she says.

At United, though, the main concern is right to access. "Our corporate philosophy is that access should be provided on a need-only basis," Lively explains. "We want to secure information from prying eyes."

Deciding who the company wants to protect its data from is one factor in determining the type of security controls it needs to implement. However, before managers look at who gets access, they need to look at what they want to protect and what they want to protect it from, analysts agree.

First, managers have to evaluate the assets they want to protect, says Wayne Cerow of Phoenix-based Cerow Investigation and Consultants. Some information is less valuable, and managers should not establish several password layers across the board.

For example, "tutorial games don't need four or five levels of security," Cerow says. Managers should not establish blanket security for the corporation, concurs Dipankar Basu, manager of marketing research for NCR Corp. in Dayton, Ohio. Instead, they need to examine users' security needs from department to department.

Limitations on access

After deciding what they want protected, managers then have to determine the type of access they want users to have, according to Lynch, who lists three types of limitations.

MIS managers have to decide who can access the computer system, who can see the data and who can alter the data. As a minimum requirement, he advises, "Make sure that the people who use the system are known to you."

MIS should also realize that controlling access is more difficult in some computing environments than others. Mainframe and minicomputer time-share systems provide logınn features that allow MIS to control and monitor users accessing a computer, Lynch says.

"Most local-area networks [LAN] do not [have these features] unless they have a file server." With a file server, he notes, "the LAN becomes very much like a time-share system."

According to Lynch, one form of security is to limit access to whomever is physically connected to the network. However, managers often need to add security measures to maintain control over leak points in which there are external communications along the LAN, he cautions. "When you provide dial-in or dial-out facilities, modems and gateways, you need to complement security measures so everyone doesn't dial up and use the system."

> **"More and more, our company is using PCs for sensitive data. Our corporate philosophy is that access should be provided on a need-only basis. We want to secure information from prying eyes."**
>
> SUANN LIVELY
> UNITED AIRLINES INC

The nature of a company's applications also can determine the ease with which management can implement security controls. For example, the Nnrthern Trust Bank of Chicago has to limit access of remote users connected to the corporate mainframe through PCs or terminals. The bank's solution has proven simple because its MIS department already designs the software and controls the information, explains Frank Cesario, the bank's vice-president of electronic banking services.

Northern Trust has developed a security system based on password access and controlled applications. "The software only addresses a set of specific functions," Cesario reports, "so it can only access certain files," he explains.

Because this software does not have the ability to perform other tasks, Cesario notes, "it's much easier to put a fence around what users can do."

After managers examine what they want to protect and the environment it resides in, the next step is identifying from whom they want to protect the data.

Part of this process requires the DP professional to identify security concerns. "Security has two meanings," Rodgers says. One definition involves protecting systems applications from theft or destruction; the other is protecting data from corruption, he explains.

In terms of theft or tampering, most MIS managers are concerned about employees rather than outside intruders.

"Employee dishonesty is probably the chief security concern of 70% to 80% of MIS managers," notes Kenneth Bosomworth, president of International Resource Development Corp., a Norwalk, Conn.-based consulting firm.

Much of a manager's concern is born out of experience, Bosomworth claims. However, he says, "Organizations tend to be secretive about this [experience]. Most embezzlement and employee dishonesty is never specifically reported to the police." More than causing embarrassment, he explains, such internal crimes can threaten high-level managers, including the company president.

Unintentional errors

In protecting against data corruption, managers are generally concerned about user errors. For example, United's security measures were designed for inexperienced users as well as high-tech intruders. "As people are brought into new departments, they are being exposed to personal computers for the first time," United's Lively explains. "We want to guard against them making unintentional errors."

Equally important is making sure that the right people use the computer "One problem with security is that users often get frustrated because it's difficult for them to get the data they need," NCR's Basu comments.

Such frustration can lead to users simply not utilizing the system or, worse, not using the security properly, Rodgers explains.

Users will commonly adapt to a hard-to-access system by creating computer crib notes, Rodgers says. "People will literally tape their passwords or logon procedures onto their monitors or put them in an adjacent drawer," he explains. Such practices can neutralize the effectiveness of a security system costing several thousand dollars, Rodgers asserts.

"You can tell users not to write down their passwords, but they still will," Bosomworth adds. "People usually choose words such as the name of their dogs. These are not unusually hard to memorize, but users will write them down anyway"

Security does not have to be difficult, however. There are several technological solutions that simplify security measures from the user's perspective In micro-computer-to-mainframe links, the software should provide all logical security, according to Basu.

"Users should only have to type in an identification and a password," Basu maintains. "The product should not require a lot of user training."

At United, MIS has combined password access with encryption to provide personal computer users with easy communications to the company's central processor. "We allow users to select their own passwords because the tendency to paste them up is much less likely," Lively says. Users require these passwords to unscramble certain encrypted files

So far, the system has effectively met United's needs, Lively states. "We anticipated that users would forget their passwords, but in the past 1½ years, this has occurred only two times," she reports. When users forget their passwords, MIS has a backup recovery system with a master key to users' files, and "recovery takes just a few seconds," Lively notes.

> **"People usually choose [passwords] such as the name of their dogs. These are not unusually hard to memorize, but users will write them down anyway."**
>
> KENNETH BOSOMWORTH
> INTERNATIONAL RESOURCE OEVELOPMENT

Sophisticated micro-to-mainframe products will also provide a script facility that MIS can use to write in the mainframe logon procedures, Rogers says. Using these scripts, a user can enter a password, which activates the logon process.

Problems in overnight transfers

The problem with such features, Cerow comments, is that they also make it easier to break into the system. "If users have to do an overnight transfer, they have to leave their password on the screen where anyone can see it," Rodgers concurs.

One solution developed by On-Line Business Systems is a means for hiding the password in the code of Excellink, the firm's micro-to-mainframe product. When users initiate an overnight transfer, the password disappears from the screen and is stored in Excellink as data, Rodgers explains. To locate the password, a user would have to know the code for both Excellink and Microsoft Corp.'s MS-DOS, he reports. "That's a virtually impossible task."

Some easy-to-use security devices vendors are touting are ID cards that users can pop into their systems, voice recognition products and scanners that identify fingerprints or the unique pattern of blood in the retinal wall of the user's eye.

However, these solutions do not have many real-world applications, according

to many experts.

ID cards are easy to use, Rodgers acknowledges, but they also can be easily lost or stolen.

Retinal vessel patterns are not susceptible to duplication, according to a recent International Resource Development report on security, but the study's findings question whether many people will be comfortable subjecting their eyes to an infrared scan. Additionally, such scanning devices cost more than people are willing to pay, according to Advanced Computing's Lynch.

'People are cost-sensitive'

In fact, DP managers apparently are reluctant to implement even the more traditional forms of security. "People are cost-sensitive," Lynch comments. "Enough users will have to lose big before they decide that security is worth the extra cost."

Thus, vendors such as Sun Microsystems, Inc. of Mountain View, Calif., are often far ahead of market demand. "Sun has built in a space for a cryptology chip in its workstations," Lynch notes, "but no one's asking to have one plugged in."

A more cost-effective approach to balancing ease of use with security is the dedication of management resources. The obvious tactic for managers is to educate users on proper security practices, according to Rodgers.

"Perfectly good passwords have to be changed frequently because of users' carelessness," he asserts. Managers need to encourage users not to write down their passwords or leave them on the screen when they are at lunch, Rodgers says.

"Employees are basically honest," Cerow explains. "If managers make employees aware of security practices and their importance, they are less likely to inadvertently give off a password or leave their terminals unattended."

The end user's awareness is a very inexpensive security measure, but it is not effective without backing from top management. "A company has to develop the policies and procedures for security before it can expect employees to follow," Cerow adds.

Ultimately, then, the management of security rests on MIS. However, MIS often has not given security its full attention. Sometimes MIS takes shortcuts in developing and implementing an application, Rodgers says.

For example, it is critical for the accounts payable software to be up and running, but initially, MIS does not need to complete the documentation.

Similarly, he says, the application doesn't need security features to work. Because of deadline demands, MIS tends to implement these measures after the fact. "That's the reason why MIS is not very good about security," Rodgers concludes.

Interest on the upswing

In the past few years, though, MIS has begun devoting more attention and resources to security, Rodgers acknowledges.

Reasons for this interest include the increasing use of micro-to-mainframe links and their attendant security problems as well as a heightened awareness of security breaches, he says. "I can recall one company in which security was not an issue until a board member read about a $50,000 embezzlement in *The Wall Street Journal*," Rodgers says.

Though security has caught MIS's attention, it may be a few years before system managers implement solutions.

According to Rodgers, MIS managers don't want to choose products and policies that only solve half of their security problems. Until they find the combination that provides a complete solution, they will not move ahead. "That's why MIS does not yet have all its security ducks in a row," Rodgers says. ❖

Tinker, tailor, network spy

BY JOHN VACCA

The increasing popularity and population of micros present many problems and risks for MIS. With systems spread among a variety of users, far from MIS's supervision, micro users can easily inflict serious damage to a network either through unwitting misuse or through intentional fraud or sabotage. As companies replace dumb terminals with micros to allow mainframe access and help mitigate the data processing burden, the potential for network security problems and risks increases.

Companies can minimize the chance of intrusion through protective devices and procedures and through ensuring that if a break-in does happen, it will be detected as soon as possible. It can also be detected through reconstructing the status, control information and content of any transaction at the time of the intrusion as well as all operator interventions that may have altered the oetwork configuration.

What are some of the risks of which MIS managers should be aware?

A person can wiretap or tamper with circuits and switching nodes with modest technical training. Eveo in-house sites, which should be the easiest to secure, are often unprotected, having exposed telecommunications cable terminations. Intruders can connect a tap out of sight via a small isolation transformer behind a termination panel that connects to another line at the end of which they can operate in comfort.

Off the premises, a tap can be placed along any part of a terrestrial link — microwave tower to tower or land line. If the intrusion is well-hidden, a company might never discover it unless it traced the entire physical path of the link. And, even then, such a discovery would only mean detachment of the device, not apprehension of the thief.

Satellite down links are especially vulnerable to electronic interception. A pbysically attached device is not required; a receive-only earth station anywhere within the footprint of the signal, which may consist of thousands of square miles, combined with a transmit device, can read, alter and reenter information without the sender's or receiver's knowledge.

Electronic eavesdropping, in turn, may reveal information sucb as passwords and account numbers that will open up a new range of fraudulent opportunities for an intruder.

What can MIS do to discover, thwart and prevent network security problems? Many hardware and software products on the market can increase network security, but both experts and users generally agree that technical solutions are not enough. The reason is simple: The people who use the network system — the ones most likely to damage or abuse it — will also know about the system's safeguards.

"The majority of white-collar crime is committed by insiders," says Frederic Withington, vice-presideot of information systems at Arthur D. Little, Inc., a Cambridge, Mass.-based consulting firm. "No technical gimmick for stopping [access] will work if the people who know the gimmick commit the crime," he says.

Even if users are not trying to abuse the network system, many of them will ignore security procedures, notes Martin Kalin, a senior associate with the Technology Analysis Group, Inc., a research firm in Washington, D.C. "Many commercial network systems aren't used properly, and people are sloppy in their daily habits

JULIA TALCOTT

Vacca is a free-lance technical data processing and air and space contract writer based in Topeka, Kan.

or not trained properly." he says. "So, it becomes a question of managing the protective network system, nnt the system itself"

Therefnre, the keys to security are not only effective MIS management but also effective personnel management. Most experts recommend a variety of technical and managerial actions, including the following:

- Encryption In 1977, the U.S. Bureau of Standards adopted the Data Encryption Standard (DES). DES defines a fixed-transformation, nr scrambling, algorithm varied by a key.
- Key management. Key creation, assignment, distributinn and cancellation are the most exposed parts of the encryption process. Management can be either manual or automatic.

A secure combination of manual and limited-automatic key management is to have different employees independently generate two preliminary keys that are separately entered into a cryptor that supports this process. The device then cnmbines them intn the final key. No one ever sees the final key; it is stored in the device and cannnt be read out The preliminary keys would also be separately delivered to the sites.

- Authentication Authentication is to a message what a parity bit is to a character nr what a block check character (BCC) is to a data block. If the parity bit, BCC or authentication field calculated at the sending side and added to the message cannot be recalculated on the receiving side tn match, then the incoming message is not released or files updated until verification is correct. Typically, retransmission is requested or other recovery procedures are undertaken.
- Terminal sequence numbers. What is the most direct way to detect message loss, duplication or fraudulent insertion of a message onto a line? The answer is to use sequence numbers on a per-terminal (meaning anything from a teletypewriter to a computer) basis. Each message sent in a terminal-to-host direction would carry its own increasing number in an input sequence number field generated automatically by a binary counter.
- Passwords and log codes. A password is what a person uses to get into the system, and a log code is what a terminal uses tn do the same. Each is a prestored secret symbol set that must be matched before a machine allows a user further access. Password/log code implementation can range from single-level to a pyramid-type construction, in which passing one level merely leads to the next.

Passwords can be used to restrict access to various systems function/transactinn classes so that only users owning those passwords can access the function.. and classes.

There are also various defense measures for terminals that companies can use tn safeguard valuable information, such as the following

- Hardware protocol verification. This technique helps to ensure that the host is in contact with tbe right ıerminal
- Physical vs logical check This security measure allows the host to validate the symbolic against the entering port and the terminal symbolic against the hardware ID of the hardware protocol verification
- Message checks The host should do message checks such as transaction type, date and minimum and maximum limits on fields in which specific content is not defined. An intruder would have to know correct formats to get through.
- The performance of close-the-loop functions at the logical level. This activity means each action would have an acknowledgement
- Employee honesty. What is to stop a person with proper password authorization from downloading a client list to diskette and passing it to a cnmpetitor? There really is no good answer beyond careful password management, but two other defenses are possible — using diskless workstations and keeping sensitive files encrypted in the host and, upon proper password, downloading them without decoding
- The definition of nonexistent terminals. Are nonexistent terminals predefined in system tables? If so, the potential risk is that an intruder terminal could be attached as a predefined identity. The best way to handle this is to ensure that these terminals are cut off in some other way such as by password control.
- Knowing the system. MIS managers need to know the network security features, such as CICS, that their teleprocessing monitors support.

Automated checks are no substitute for operational precautions and awareness. Telecommunications security grows from a careful mix of computerized and manual procedures

To prevent unauthorized access, MIS should assign terminal areas their own dedicated secure space; keep test keys and signature lists out of the way; place supervisor's office in view of the work area; and so on. It should consider terminal locks and magnetic card slots for operator identification.

Furthermore, MIS needs to be aware of network status. The network is always in flux; carriers fail and are restored, terminals may not respood to poll/selects or may be logically disabled and so on. Greater risks accrue during abnormal operation, especially if the malfunctions go undetected. Therefore, network implementation, including software, should build in functions to detect malfunctions and alert MIS

MIS may also want to separate functions. The principle here is that collusion becomes more difficult as more people become involved. Therefore, where it is consistent with smooth work flow, different people should do different parts of an operation.

An item-by-item reconciliation should be conducted, not for the purpose of prevention but for detection of any lost or altered data soon after the fact.

MIS should reconcile cross-checks and summaries. This method divides into operations and applications. For operations, include periodic communications between terminals, the exchange of reports of message types and counts received for comparison. For applications, include daily dollar totals and the number of messages the system accepts compared with the dollar total and number of messages it delivers, plus those still in the queue.

MIS must keep information private. Knowledge of controls, tests for failures and the like should be limited to a minimum number of personnel.

Also, MIS should institute audit trails. The purpose of audit trails is to allow a person to reconstruct in sequence all actions and interventions that affected system components and states up to a given time. Audit trails also trace the progress of any transaction throughout its lifetime in the system including each node, part and terminal through which it passed, noting any special delivery conditions and auxiliary messages generated.

Much of the concern for network security is placed on protecting access to the mainframe and its data base, but with increasing demands to use that data on PCs, local-area network (LAN) security is also a pertinent issue. Ron Kopek, president of Edge-Tech Associates, a San Francisco-based consulting firm specializing in PC-to-mainframe communications, points out that once data is transferred from the host, all central control is lost.

In this environment, the PC is an attractive target for data theft, sabotage and extortion. The integration of PCs and teleprocessing networks has increased the scope of the problem.

Continued on page 44

A smarter smart card

Networks pose special security problems. Security decreases as the number of system users increases, and networks, by definition, exist to give access to a lot of people

The first challenge in maintaining security is to keep out anyone who doesn't belong on the network. Various methods exist that perform this function, most of them involving some combination of passwords and, increasingly, pass cards, magoetic strip cards or newer smart cards with password information encoded un a chip.

All such methods have one drawback Anyone who gets his hands on the card and learns the password can get into the network

Smart card + password control

One variation on the smart card shows promise, however The Challenger card, developed by Sytek, Inc., in Mountain View, Calif., in conjunction with the British firm Open Computer Security, was designed specifically as an internal security tool for operators of private networks, combining the smart card method with a type of password control. This control consists of two components: a central unit that attaches to the main computer processor and a unit that looks like a pocket calculator with a keyboard and display.

When a user logs on with a password, the system issues him a random number. The user then punches another password into the calculator unit, which asks for the random number The unit encodes that number and displays a scrambled version. The user then punches this version into the network, where it is decoded.

An unauthorized user, therefore, has to know the calculator's password, the system's password and must get by the calculator unit to get into the system. Without all three, he is, in effect, confronted by a new password — the random number issued by the system — each time he tries to gain access. To prevent determined hackers from automatically dialing an endless string of random numbers, the calculator freezes after a user punches in three wrong numbers.

Protecting networks against unauthorized users, as is the case with single computer systems, does not protect against authorized users bent on mischief, however. In addition, the management techniques that may solve a single installation's problems are less effective when applied to a network because of the number of users, many of whom may be a continent away.

The solution seems to lie in a combination of encryption, passwords and strict levels of access. Corporate users, especially those in the defense industry, are taking increasing interest in government network security ratings. As more corporations demand computers and networks that meet government standards, vendors will be forced to build security into their products, and systems and network managers will have to devise policies that make those security measures work. — JOHN VACCA

Spy

Continued from page 43

However, Kopek says he believes that users generally have to solve network security problems on their own. He recommends a needs assessment, including a review of mainframe software and expected PC-based applications, before the installation of a PC-to-mainframe link

In one research corporation, encryption packages have been made available for all PCs "We make sure users understand that data in a PC is much more public than data in a host computer, but it's up to the individual users to employ the package," says the firm's MIS department head, who asked not to be named.

Although hackers don't present the greatest danger to network security, users are still concerned with that threat. For this type of security breach, analysts recommend various technical solutions.

Any communications link involving PCs — even between the PCs themselves — essentially broadcasts the data being processed or transmitted because outside sources can easily monitor the electromagnetic emissions. Shielded cables and equipment and data encryption are the only ways to prevent this breach.

Protection is a little trickier for unshielded satellite transmissions. On the residential market side, effective scrambling of a satellite television signal is imperative if the cable industry is to survive or succeed with direct broadcast satellite service, also known as DBS. On the business end, the proliferation of videoteleconferencing and business television broadcasts necessitates enhanced encryption techniques to protect sensitive corporate information.

It is vital that satellite suppliers concentrate on the issue of network security. Generally, the only deterrent is well-planned prevention.

What then, will the future hold for satellite transmission security? Some of the technologies either being refined or soon to be introduced include the following:

- Digital processing techniques for scrambling each video line and/or eliminating all synchronizing information within the horizontal and vertical blanking intervals of the signals.
- Combined technologies utilizing encrypted uplinking for pay-per-view movies and digital audio transmission to facilitate distribution of stereo TV.
- Use of spread spectrum and time-division multiple access for sensitive information, because the likelihood of intercepting the entire message, as opposed to bits or chips of one, is remote.
- Use of spot beam or antenna beam shaping whereby down-link signals are molded either mechanically or electronically in a concentrated pattern, minimizing interference, increasing strength and reducing the chance for eavesdropping.

The concept of network security is based on an accumulation of small deterrents that, together, dissuade or intercept the most dangerous threat of all: collusion among knowledgeable insiders. But no completely secure system is possible because safeguards must also be balanced against the need to maintain work flow.

> **Network security is based on an accumulation of small deterrents that, together, dissuade or intercept the most dangerous threat of all: collusion among knowledgeable insiders.**

With this in mind, what is the future of network security?

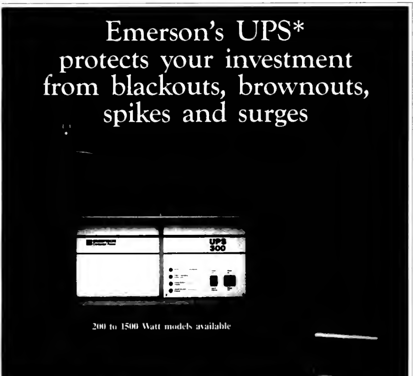
The future of network security will no doubt center on LAN gateways, internetworking and satellite transmission. Consider a future case in which one side of a computer will be interfaced to another LAN, a privately owned wide-area network or even a public switched network. This type of environment, in which multiple networks are tied together by common nodes, is referred to as an internetwork, and gateways are the common nodes that effect the interconnection.

One example of such a future configuration is a company with multiple sites, each with its own LAN, all tied together via dial-up telecommunications circuits. LAN security issues are currently compounded by the addition of dial-up lines and more authorized users who could be spread worldwide.

The network security threat in internetwork environments will continue to require increased security operations. The relaxation of local control will mean that many more parts of the network will not be trusted. When lower layer protocols cannot be trusted, then a company must place security features at the higher layers of the protocol hierarchy.

Security for satellite transmission and networks is merely another sign of the continuing integration of computer and communications technologies in contemporary information systems. It is one more step in the removal of the lines between computers and communications, and between LANs and wide-area networks.

It is important for MIS to realize that it can understand network security threats and defenses only by looking at the total information system picture. ❖



Justice and data for all

BY REBECCA HURST

Information managers will not take data base censorship lying down. That is the message the Information Industry Association and other organizations have made clear to the U.S. government by successfully challenging a policy directive from former National Security Agency director John Poindexter. In November 1986, Poindexter issued a policy giving the government power to supress information it deemed "sensitive but unclassified." This policy was based solidly on the two-year-old National Security Decision Directive (NSDD) 145 that outlined similar powers for administrative agencies. However, information industry leaders identified the policy as a threat to privacy and freedom of speech, particularly for public data bases. Shocked and indignant, they quickly brought the policy to the light of public scrutiny that lead to the policy's rescision earlier this year (see story on government regulations, page 47).

Days after Poindexter issued the directive, more than 100 members of the Information Industry Association (IIA) sat amazed as Diane Fountaine, who heads the Pentagon's information systems directorate, outlined the administration's plans.

"I was greatly distressed," recalls Kenneth Allen, the IIA's vice-president for government relations. "I thought Fountaine was going to say that the Pentagon wasn't concerned about public data bases. Instead, I heard just the opposite."

The issue was not whether the administration would protect information, Fountaine said, but what information within government and industry it would protect. Beyond this statement, though, she offered little detail. "Fountaine didn't give specific examples and wouldn't even tell us what the administration planned to do," Allen says. "I was very dissatisfied."

For Jack Simpson, who also attended that meeting, the implications became disturbingly clear. Simpson, president of Mead Data Central, a Dayton, Ohio-based supplier of such data base services as Nexis and Lexis, soon received visits from several government agencies including the U.S. Air Force, Central Intelligence Agency and Federal Bureau of Investigation, to evaluate Mead's data base service operations and suggest control methods. "The Air Force was the most confident," he observes "They asked, 'Can you do this? Can you monitor that?' "

Later, the Air Force published a report on Mead, Simpson recalls. "I asked if I could see it because it was about my company," he says. "They said I couldn't because it was classified, but they would send me an unclassified version in 90 days. It's been more than 90 days, but I still haven't seen it."

The situation has been sticky, Simpson notes. Some of Mead's best customers are from the government, including the White House, U.S. Senate and Internal Revenue Service, he says. "When something is running amok, though, someone has to say, 'This isn't right.' " Following his beliefs, Simpson agreed to speak to Congress on behalf of the IIA and Mead.

On Feb. 26, Simpson testified before the

Public outcry foiled a federal policy that limited privacy

GOVERNMENTAL CONTROLS

House Committee on Government Operations on NSDD 145 and the "sensitive but unclassified" policy and also spoke in behalf of a House of Representatives bill known as H.R. 145, or the Computer Security Act.

H.R 145, he argued, would provide a clear distinction between federal and private computer systems and between control of tbe computer systems and control of the information itself.

Simpson was not the only one who expressed concern about NSDD 145. Several organizations, including the IIA, Institute of Electrical and Electronics Engineers, Inc., American Library Association and the Association of Research Libraries testified as well.

> **Even though NSDD 145 does not provide the government with legal authority to institute information sanctions, the perception that it has this authority can be equally threatening. "The government is like a 6,000-lb gorilla. When it moves, you don't ask if it has the right to do so; you move out of the way."**
>
> KENNETH ALLEN
> INFORMATION INDUSTRY ASSOCIATION

The administration, feeling heat from Poindexter's "sensitive but unclassified" policy, also began to communicate with Congress.

On March 17, this contact culminated in Secretary of Commerce Malcolm Baldrige's testimony before the Committee on Government Operations on behalf of H.R. 145. That same day, Baldrige announced the rescission of Poindexter's directive. Calling the directive "controversial," he stated, "the procedures by which it was issued raised legitimate questions about the role of the National Security Adviser."

Repealing the policy was a step in the right direction, but many industry leaders and legal experts agree the problem has not been entirely resolved. The Poindexter policy crossed over the lines of constitutionality, explains John Yates, partner in the Atlanta law firm of Vaughan, Roach, Davis, Birch & Murphy. However, he says, "The fact that the administration rescinded the directive doesn't mean it won't try to issue one again."

The problem, Mead's Simpson claims, is that the current implementation has been stopped, but the directive that allowed it, NSDD 145, is still in place. Even though NSDD 145 does not actually provide the government with the legal authority to institute information sanctions, IIA's Allen warns, the perception that it has this authority can be equally threatening. "The government is like a 6,000-lb gorilla," he says. "When it moves, you don't ask if it has the right to do so; you move out of the way."

The directive, NSDD 145, primarily defines organizations and policies for maintaining standards for cryptology, telecommunications and automated information systems security. However, it also seeks to identify categories of sensitive nongovernment information and recommend steps to protect it.

"In cases where implementation of security measures to nongovernment systems would be in the national security interest," the directive says, "the private sector shall be encouraged, advised and, where appropriate, assisted in undertaking the application of such measures."

Further, while NSDD 145 was designed to regulate and monitor private information, the systems security group responsible for implementing the directive has no c vilian representatives.

Instead, the group consists of the secretary of state, secretary of the treasury, secretary of defense, attorney general, director of the Office of Management and Budget, the director of central intelligence and the assistant to the president for National Security Affairs, who chairs the group.

Consolidating security

The directive was initially intended to consolidate security under one head so that it would be cohesive, according to Ed Zeitler, vice-president and manager of information systems security at Security Pacific National Bank in Glendale, Calif. "That was a very good thought," he says. However, Zeitler explains, the standards that are fine for the government are not entirely appropriate for the public sector.

The policy is too broad, Mead's Simpson concurs. NSDD 145 was designed to cover three levels of security. However, it should only concentrate on the two that describe government agencies, he argues.

The first level is classified information in such agencies as the defense department, the CIA and embassies, Simpson says.

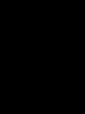
The second level covers civilian federal agencies including the IRS. These organizations do not have heavily classified information, but some of it is sensitive, he notes. "You don't want just anyone getting into tax returns."

Continued on page 48

Start your subscription now, and save $9!

JUST 69¢ AN ISSUE

For over 20 years, COMPUTERWORLD has covered the ever-changing field of information systems like no one else. And we're moving into the next generation of technological advances with an expanded staff, more features, and the same determination to keep you on top—and slightly ahead—of new developments. Join the celebration! One full year (51 issues) costs just $35, a savings of $9 off the basic rate, and only 69¢ an issue!



PLUS 12 BONUS ISSUES

When you subscribe to COMPUTERWORLD, you also get 12 monthly issues of Computerworld Focus, FREE. Each issue covers one particular topic—in depth. Topics include microcomputing, communications, software, connectivity, and much, much more. Leading edge information —for subscribers only!

PLUS A FREE MAGIC MUG

What's a 20th Anniversary Celebration without something to remember it by? This unique COMPUTERWORLD coffee mug features a special "magic message" when it's filled with a hot liquid. And it's *yours free* with your paid subscription to COMPUTERWORLD.

Subscribe today by returning the order form in this postage-paid envelope now!

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST CLASS PERMIT NO 55 NEPTUNE NJ 07754

POSTAGE WILL BE PAID BY ADDRESSEE

CIRCULATION DEPARTMENT
COMPUTERWORLD
P O Box 1565
Neptune NJ 07754-9916

GOVERNMENTAL CONTROLS

DES gets an encore

March signaled a shift in governmental power over private security. A victory for the U.S. private sector unfolded as the National Security Agency (NSA) overturned its previous statement of direction and agreed to support the Data Encryption Standard (DES) — at least for a few years.

A year and a half earlier, the NSA had announced that it would not renew its endorsement of DES. Instead, the agency planned to replace DES with an encryption standard developed under its Commercial Comsec Endorsement Program (CCEP). The NSA's decision was not directly tied to the National Security Decision Directive (NSDD) 145, says Kenneth Allen, vice-president for the Information Industry Association (IIA). However, it signaled another attempt from the government to regulate sensitive but unclassified information.

The NSA's standards announcement quickly raised questions, concerns and outcries from the financial industry.

"The NSA was attempting to withdraw DES without regard for the economic impact it would have on U.S. business," IIA's Allen comments. Replacing DES-based security equipment without a transition period would be expensive, concurs Ed Zeitler, vice-president of information systems security at Glendale, Calif.-based Security Pacific National Bank. Zeitler also serves as a liaison between the NSA and the American Bankers Association (ABA), a Washington-D.C., organization that represents 95% of U.S. commercial banks.

The ABA has found other expenses related to the NSA's policy, Zeitler says. While some of the CCEP algorithms are applicable to part of banking's processing, they are too expensive to justify using in other areas. In addition, the NSA wants to generate and manage the keys that decrypt these CCEP security systems. "If we had to go to the NSA, the cost overhead would be too high, and it would limit our use of equipment," he says.

The keys to the kingdom

However, the greater issue of key management is the NSA's ability to assign access to private businesses, industry watchers agree. First, if the NSA generates the keys for private businesses, it will potentially have access to those companies' data bases. Second, businesses are ultimately responsible for their own transactions and data bases. Therefore, they should have control over securing them, Zeitler asserts.

Another problem is that many firms need to perform transactions with foreign businesses. DES is available to many foreign countries, but the CCEP algorithm would not be. Even if it were, Zeitler notes, "I'm not sure how well a government-owned algorithm would be accepted by foreign businesses."

Finally, the agency has shifted its development focus, according to Kurt Barker, an analyst with Trusted Information Systems, Inc. of Glenwood, Md. Originally, the NSA had concentrated on Type 2 algorithm modules designed for sensitive but unclassified information. These modules would affect private industry, Barker says. The NSA has since shifted its emphasis to algorithm modules for classified data, which would primarily be used by the government, he comments.

Without a fully developed set of algorithms from the NSA, DES is the only encryption standard that businesses have, Zeitler says. "The fact that DES is a nationally recognized standard has made a big difference in industry," he asserts. "Without DES, we would be at the mercy of the vendors."

The NSA, realizing that it cannot address certain technical and management issues, has agreed to endorse DES for another five-year period while it continues to work on its CCEP algorithms.

For its part, the ABA has announced that it will already work with the NSA to develop standard algorithms that will meet the needs of private business as well as government. Already, the banking association has sent the NSA a list of suggestions for a workable encryption standard, including the following:

- The encryption code has to be available for international transactions.
- CCEP needs to be verified by an independent resource.
- Government certification should remain under the domain of the National Bureau of Standards while the NSA develops the code.
- The encryption standard has to work with multiple vendors' equipment and provide multiple translations.
- The encryption standard has to be compatible with existing communications security technology, notably American National Standards Institute standards
- Private business should be responsible for key generation and management because it is held accountable.

Much of the ABA's concerns are political ones that will pose a sticky problem for a number of years, Barker asserts. "It will be tough to find a replacement for the DES algorithm," Zeitler concurs. However, he says, "[the NSA] has been very responsive and is attempting to come up with solutions that meet our needs." — REBECCA HURST

Justice and data

Continued from page 46

The third level is public, nonclassified data "This is information you can find in *The New York Times, The Wall Street Journal* ur Nexis," Simpson explains. When the government is looking at Levels 1 or 2, it's obvious for NSDD 14S to talk about protecting information," he asserts "When NSDD 14S tries to apply that control to the third layer, that's a problem." Trying to control public information not only violates the rights of free speech and privacy, Simpson argues, it also exceeds the work load the government is capable of handling

Instead of putting energy into the private sector, he says, the government should concentrate on its own internal security. "The core of the government's security system is in disarray. Look at what's happening at our embassies," Simpson notes.

A solution in H.R. 145

Many observers agree the solution is to distinguish between control of government agencies and the public sector by redefining or eliminating NSDD 145 and by passing H.R. 145 into law. As a law, H.R. 145 would take precedence over NSDD 145 and place computer security in the hands of civilian agencies, IIA's Allen notes.

Already, the administration has begun reviewing NSDD 145 "to resolve any ambiguities in that document with respect to the role the National Security Adviser will play in the future," Baldrige stated in his March address. He also announced the administration's support for the Computer Security Act, H.R. 14S. "Good legislation in this area," he said, "will foster the progress we want to achieve in enhancing the security of federal government systems."

"H.R 14S has a much narrower scope than NSDD 14S," Simpson comments. "It doesn't talk about information classifications." Instead the Computer Security Act takes a two-pronged approach to securing computer systems.

First, the bill reaffirms that the National Bureau of Standards (NBS) is the governmental agency responsible for developing standards and guidelines for computer systems, including those for security.

H.R. 145 also states that NBS will develop guidelines for training federal employees about "security awareness and accepted security practice." In addition to these duties, NBS is authorized to assist the private sector in using and applying the results of these programs and activities.

Second, H.R. 145 seeks to establish a Computer System Security and Privacy Advisory Board within the Department of Commerce that would represent both the government and private industry. The proposed group would consist of eight nongovernment representatives who are eminent in the computer or telecommunications industry and four members of the federal government who have systems management experience. In addition, there would be a chairman appointed by the Secretary of Commerce.

This board would serve three primary functions:

- To identify emerging managerial, technical, administrative and physical safeguard issues relative to computer systems security and privacy.
- To advise the NBS and the Secretary of Commerce on security privacy issues pertaining to federal systems.
- To report its findings to the Secretary of Commerce, the director of the Office of Management and Budget, the director of the National Security Agency (NSA) and the appropriate committees of Congress.

However, H.R. 145 is not in its final form. Changes to the bill can be expected because the administration only supports it witb some modifications, which Baldrige outlined before Congress in his March speech.

To clear the air over the "sensitive but unclassified" directive, the administration is calling for "clear language to the effect that nothing in this bill authorizes the government to withhold information that is otherwise available to the public," he said.

A presidentiol review

At the same time, the administration called for provisions for presidential review of standards and cooperation between the NBS and the NSA. These provisions were designed to assure that NBS standards are consistent with national security use technical guidelines from the NSA.

Finally, the administration wants to drop the portion of the bill that creates the Computer Security and Privacy Advisory Board. Instead, it prefers to "make training in computer security a direct responsibility of agencies," Baldrige stated.

Simpson also would like to see changes to the Computer Security Act. "It's a good start," he claims, "but H.R. 145 needs two more pieces before it effectively counteracts the national security directive." First, the bill needs to explicitly describe what controls, if any, the government can implement. Second, he says, H.R. 145 must define whether Level 2, nonclassified federal information, needs to be regulated as well as computer systems. If these changes are made, "then the government wouldn't need NSDD 145," Simpson asserts. ❖

EFT PROTECTION

It's in the bank... or is it?

BY ROBERT DRATCH

Jesse James and his band of bank-robbing hoodlums are part of folklore. Today, however, the infamous practice of robbing banks has taken on more meaning than just holding up a teller for a sackful of coins. Rather, tapping into the sophisticated electronic exchange systems that are an integral part of modern banking is tantamount to a holdup of far-reaching consequences.

Banks have a long history of being very concerned and cautious about protecting customers' proprietary information — such as balances, valuations of financial worth and value-bearing transactions, including money transfers and other customer financial activities. Banks have always provided extensive controls to protect information and transactions in paper form.

Examples of these controls include signature verification/authorization; telephone callback to customers to check the authenticity of the sender and the integrity of the contents of funds transfers sent by wire or mail; and cameras and alarm systems to protect bank branches and automated teller machines.

Today, as the handling of information in electronic form becomes more and more a part of banking, the banking industry is pioneering new ways to use computer-based technology to secure financial transactions.

Three major areas of data security in the banking sector have emerged over the years: access to systems, message integrity and privacy. For about 10 years, access was a primary focus in addressing security issues. Security measures first started with time-sharing vendors, in which customers were identified at the access level with particular user identification and passwords.

The major areas of concern in sending a transaction have traditionally been the customer's office, the network and the bank. Within access there should be implied rights in the transaction process based on whether you are a customer, a bank employee or someone else.

The best technologies currently available for securing financial transactions are those based on cryptographic techniques. Cryptographic hardware and software have been commercially available for more than 10 years in the U.S., and application of these techniques in the nonbank private sector has been scant.

As technology grew more sophisticated, message integrity became a key focus of data security. To preserve the integrity of a message, the authentication process establishes the message's validity or verifies a user's authorization for access to data. Authentication uses cryptography to verify the authenticity of the sender and to ensure that no alteration has taken place in the contents of the information sent by an authorized sender.

The banking industry, as well

Dratch is vice-president and manager of management control and data security for global electronic banking at Chase Manhattan Bank NA in New York

as many segments of the corporate marketplace (for example, manufacturing and broker/dealers), are establishing requirements to use authentication and encryption — a scrambling technique for disguising a message at its source and unscrambling the communication at its destination — to protect the movement of valuable information between enterprises.

This movement is facilitated by the existence of standards developed under the aegis of the American National Standards Institute (ANSI) with assistance from trade associations such as the American Bankers Association.

Standards provide direction

Standards on authentication and encryption have provided technical direction to vendors in developing hardware and software components to support these methods of securing data. In turn, key management has become important to the security of the whole process

At first, test keys were used for authorization. Now, the authentication standard for financial messages established by ANSI relies on the Data Encryption Standard (DES) algorithm to produce a message authentication code (MAC). The authentication process uses a secret key, or value.

This key as well as the data in the message being sent are fed into the authentication algorithm. The end result is a MAC that is highly unique for that key and that particular message. If the key is wrong or the message has changed, the MAC will be invalid. This process can be done in software or hardware and is routinely employed by Chase Manhattan Bank NA in all its personal computer-based transaction initiation products delivered to corporate and institutional customers.

Data security cannot be effective without physical security.

To ensure that information cannot be modified, message authentication applies a unique MAC code at the end of the transaction based on the value of the information in the transaction. Authentication can be used for stored data as well as data moving across the network.

Once the data is sent by the customer to the bank, authenticatioo serves to secure the data both during transmission and while it is stored. Most money center banks — banks that handle global financial exchanges — are extending their use of authentication, both internally as well as externally, with customer interfaces.

Use of authentication has become so prevalent that even the Department of the Treasury, for example, has issued a directive requiring ANSI message authentication for its own internal systems, and the Society for Worldwide Interbank Financial Telecommunications employs both authentication and encryption as standard features of its system.

Privacy issue

In banking, another area of concern in the evolution of data security is the privacy issue.

To ensure the privacy of a message, many banks use data encryption. Encryption disguises the contents of the information, allowing only the authorized user to translate scrambled information into readable form. Encryption systems that work at the word level are called code systems, while the systems that work at the number or letter level are called cipher systems.

Encryption can also be used for transmitting information, such as in the case of a money transfer. Using this encryption method, customers can prevent the viewing of data during transmission as well as when the information is stnred in their own systems.

Sensitive information such as customer passwords and personal identification numbers are routinely encrypted on files and in computer networks. Critical communications links between intrabank computers and Federal Reserve Bank computers are also protected with encryptinn.

Cipher process

Encryption uses a cipher process similar to authentication in which a secret key, such as a code or password, makes the result unique for the user. Both encryption and authentication follow specific mathematical formulas. The algorithm is the same for both and generates two types of results — encrypted data and a MAC for data.

Chase Manhattan Bank is currently building the capability to both authenticate and encrypt for a single money transfer between bank and customer, utilizing all three types of controls — access, integrity and privacy.

In addition, different types of controls, when combined with authentication, allow a user to eliminate duplicates in a network environment. Authentication alone will not allow banks to detect duplicate transactions resulting from an active wiretap.

However, additional measures such as date-stamping the transaction or giving it a sequence number at the customer's location will allow officials to check for duplicates on the bank's side.

By including sequence oumbers and dates in the authentication process, the bank can tell if a transaction has been duplicated or oot. If someone were tampering with a transaction, the MAC validation would fail. Combining these integrity controls provides a more secure transaction

Vulnerable environments

Of the three environments — in the customer's office, in the network transmission or at the bank — in which a security breach may occur, the network poses the least threat of being penetrated. The customer's office and the bank environment hold the greatest potential for being the areas in which to violate a transaction because the greatest expertise in technology and operations exists at those two points.

Separation of duties, for example, dividing the responsibilities for initiating a money transfer transaction among several individuals, is important in preventing breaches of security.

Physical security, of course, is another valuable method to protect data integrity. It is not advisable, for example, to write passwords down or keep a diskette with a secret cipher key on it unlocked and available.

Data security cannot be effective without physical security.

In the past three years, technology has moved rapidly, supporting multiple modes and levels of security. One of the biggest accomplishments has been to make customers aware of the need for security.

By implementing more sophisticated security techniques, banks will continue to be leaders in the deployment of computer-based technology to effect financial transaction and information flows. This technology will also be used to provide state-of-the-art security to protect crucial customer and bank data, both inside and outside the bank environment. ✧

products

TECH TALK

Barricade your company from hackers, terrorists

By Michael Tucker

When we think about protecting a high-tech resource like a computer, most of us have a habit of thinking that the threats we face are themselves high-tech.

But, in fact, a single terrorist with a few pounds of plastique can do more damage in the twinkling of an eye than an army of hackers can do in a decade.

Last November, terrorists reportedly planted a bomb in IBM's European Networking Center in Heidelberg, West Germany. No one was burt, but the blast damaged the center's mainframe and caused more than a million and half dollar's worth of damage to the facility.

Examples like that one are the reason wby this month's Tech Talk is about something old — the design of secure installations. What is new about the subject is an emerging awareness on the part of the industry that data must be protected physically as well as electronically.

That level of physical protection can be very sophisticated indeed. Sygnetron Production Systems, Inc. in Timonium, Md., is a security consultancy and security system integrator. It has oot been traditionally involved with data processing.

Check out *Focus's* Hot Seat, a new column starting this month on page 56.

"Our work is largely for the Department of Energy, the nuclear industry and large commercial installations that have connections with one or both of the first two," explains Neil Owens, director of marketing for the company.

In short, Sygnetron does most of its work in places where a breach of security could have horrific consequences. The firm defends against such things as the theft of fissionable material by terrorist groups. But suppose data was considered no less valuable (or dangerous) than plutonium, which, in a sense, it is. How would Sygnetron protect a data center?

"First," Owens says, "we'd determine the kind of assets you have. In the case of information, you have a severe security problem because it's so compact. You can steal a lot of it in a small package."

He notes, for instance, that the oew generation of write-once, read-many disks, with their vast storage capacities, makes it easy for a thief to walk out of a DP installation with a company's entire data base tucked in a coat pocket.

The outside perimeter

After determining a company's assets, Owens explains, "We'd take a look at your outside perimeter." The fence around a building can determine the structure's life or death.

"If you have a terrorist threat, for instance, we'd suggest that you have a physical barrier to keep anybody with a bomb away from the building entirely. You'd want a specialized security fence to keep a BMW loaded with TNT from ramming the wall of the data center," be says.

Only after that precaution would Sygnetron begin to consider electronic countermeasures.

At the heart of a company's system would be a host security computer, extensively interconnected with building and perimeter sensors. This machine would provide a constant overview of the area's status, maintain an extensive log of security-related events and even offer decision support functions for human guards.

"Uniformly," Owens says, "our systems are based on a host computer. Basically, you have a choice. You either go with human guards or you go with electronics. In general, guards are more expensive, and they are subject to human error. Electronics systems aren't. You're not going to compromise them with candy."

Owens suggests a dual system — various intrusion-detection sensors such as alarms, motion detectors, ultrasonic sensors and the like backed up by closed circuit television. TV cameras would be installed both at the perimeter and within the building itself.

"Closed circuit TV is superb for threat assessment," Owens maintains. "It works hand in

Continued on page 53

PRODUCT CLOSE-UP

Securing PC hard disks

MIS officers have discovered from sad experience that it is easy to secure a mainframe in a data center but almost impossible to do the same for a personal computer.

PCs are designed with the primary goal of easy access for nontechnical users. To reverse that design is literally to go against the whole concept of PCs.

However, as PCs are used in more and more situations, they increasingly hold sensitive data. A PC's hard disk may now contain information vital to the survival of a company.

Modem riska

Given the distributed nature of most modern businesses, PCs must support dial-up access. In an age when executives may be working on the road, at home or from outlying offices, it is impossible to assume that the office PC will do without a modem. But, of course, modems also mean escalating security risks.

Fortunately, a number of products are now coming to market that provide some level of security for PCs. One such tool recently introduced is Onguard from United Software Security, Inc. in Vienna, Va.

Onguard will perform antitampering checks on itself and its data.

United Software Security is know primarily for its mainframe security product, Padpath Software, which is remarketed with proprietary hardware by such firms as Atalla Corp. in San Jose, Calif., and Security Dynamics, Inc. in Cambridge, Mass.

As one of the firm's first ventures into the PC market, Onguard attempts to provide mainframe-like security functions to the hard disks of PCs.

Continued on page 52

BLUE BEAT

Security scruples

Deidre Depke

A recent episode of ABC TV's high-technology adventure program, *Max Headroom*, featured a tense battle between a young hacker and a sophisticated mainframe.

In the scene, the boy wrestles with the computer's security system in an attempt to alter a specific file. Tapping furiously at his keyboard, the hacker momentarily manages to break the security system and access mainframe data.

Although *Max Headroom*'s set is a product of the '80s and the show's computer graphics are spectacular, the scene could have come from a 1960s comic book.

The show's theme is not a new one: A human mind can always triumph over a computer mind, oo matter how artificially intelligent that computer mind may be.

MIS managers must struggle against this well-accepted belief every day. They must maintain security systems that are as close to unbreachable as is technologically possible, while they battle the mind-set of disgruntled employees, outside hackers and bored users who have come to view breaking security as a high art form.

MIS must also fight corporate managers who fail to understand that inadequate security in major installations has encouraged the pastime of computer crime. After all, breaking through barriers often isn't that hard.

These challenges become greater as the computer industry moves toward connectivity

Continued on page 58

Secur ID card changes by the minute

It's about the same size as a credit card but is roughly twice as thick. That's to be expected, however, because the Secur ID card contains a lithium battery, a band of LCD readouts and a microprocessor that generates a new four- to eight-digit code that changes every minute.

Security Dynamics, Inc., a Cambridge, Mass., maker of Secur ID, claims it is the only company currently offering such a security product.

To gain access to a computer system, a Secur ID user steps up to a terminal or microcomputer that is linked to a firm's mainframe, types in a personal identification number and the code that is displayed at that moment on his card. The host computer matches the user's number to its calculation of the number displayed on his card before it allows access to the data base.

ACE behind the cards

Of course, the Secur ID card is only the front end of the Security Dynamics system. The cards, which last two years, cost $46 apiece. Security Dynamics' Access Control Encryption (ACE) system also consists of a controller that is priced according to the number of host communications ports it protects. Depending on the size of controller and number of ports secured, the price of the ACE system can range from $2,500 to $100,000. ACE software can be purchased separately for $50,000.

Security Dynamics is going after some pretty stiff mainframe-based security competition such as IBM's RACF and Top Secret from Computer Associates International, Inc.

Bob Fine, vice-president of sales and marketing at Security Dynamics, figures that although there are only a total of about 6,000 of these systems installed in the U.S., their heavy costs make for big revenue overall.

Other competition is piling in. Secur ID is part of a security category that is made up of smart cards and programmed electronic keys. "The electronic key market is wild now," explains a researcher at Dataquest, Inc. in San Jose, Calif. "It includes everything from devices that look like harmonicas to things that resemble police whistles and activate user access through sound vibrations," the researcher says. — STAN KOLODZIEJ

Circle Reader Service Number 114

Hard disks

Continued from page 51

Onguard assumes that a system uses a PC with a hard disk as a central system and users dial in to access data.

Once installed, the Onguard program allows the system manager to prevent users from reading the hard disk and from making copies of hard-disk data onto their own floppies.

Onguard reportedly can also prevent unauthorized users from getting into the system in the first place

Automatic logoff

According to the vendor, it provides passwords, automatic logoff after a set number of failed passwords, multiple levels of security and even encryption using the Data Encryption Standard algorithm.

The product will also perform a number of antitampering checks on itself and its data. With these, the system manager can detect and defend against attempts to get around the program.

Onguard requires an IBM Personal Computer XT, AT or compatible with a 800K-byte hard disk and 128K bytes of random-access memory.

The Onguard program is priced at $295. — MICHAEL TUCKER

Circle Reader Service Number 115

Tech Talk

Continued from page 51

hand with the rest of the system. If an alarm goes off — say, at some point along the fence — then a camera in that area will automatically switch on." A guard sitting at a terminal can then tell quickly whether the alarm was triggered by something innocent, perhaps a passerby dragging a hand on the fence, or by something really dangerous.

"The next level of protection is the building itself," according to Owens. To this end, Sygnetron would lock particularly at entry and exit control. The company would install a number of devices to control entry to and passage through the building. These controls would range from card identification systems in low-security areas to sophisticated biometric devices in high-security areas.

In addition to the obvious benefit of these personnel systems — systems that keep people out of places where they don't belong — these setups also instill in people a sense of discipline. Owens explains: "It is a means of making people, particularly managers, take security seriously. One can define an excellent security system and still have it fail because management does not support it."

In fact, Owens says, not taking security seriously is fatal. He points to the example of the current scandal at the U.S. embassy in Moscow. In that incident, American guards were allegedly compromised by the KGB, the Soviet secret police and intelligence agency.

"What was amazing," Owens says, "is that [the embassy staff] had alarms in all the high-security areas. But, as near as we can tell from the limited information available to us, those alarms could be [turned off] by a single guard. And, there was no log."

He argues that there should have been multiple security stations in the embassy so that alarms could be deactivated only through the cooperation of two or more guards — in different locations — who preferably did not know each other personally. In addition, Owens says, the embassy should have had some sort of automatic recording system that would note the time at which alarms were shut off.

The log would then be reviewed on a regular basis by high-ranking embassy officers. Frequent and unexplained deactivations of the alarms would thus be noticed.

But there was no log to tip anyone off. It was only after one of the suspects turned himself in that the authorities realized something was wrong. And, if Owens is right and embassy management did not take security seriously, then the results of the security breach could be very serious indeed.

While the average MIS officer probably does not protect data as vital as that contained at the U.S. embassy, Owens's recounting of the story is still instructive.

Like Bonnie and Clyde

In the embassy case, data security was compromised by nothing high tech, not encryption-busting code masters but rather by threats, seduction, human error and breaking and entering The U.S. embassy was brought down by nothing more sophisticated than the tools Bonnie and Clyde could have applied to robbing banks in the 1930s.

Educating non-data processing management about those physical threats could be important for MIS — even vital. After all, even the most sophisticated password system or method of encryption could not have stopped that bomb in the IBM data center.

If senior management seems to believe that data security is strictly a computer problem, then it may be MIS's responsibility to see that a bit of storytelling is in order. Next time, when you have to talk to senior management and the board about security, take just a moment to show them the wall of your data center. Then, invite them to exercise their imaginations.

Safe protects in 1,700°F heat

What would happen to your company if every piece of significant data was destroyed in one day? What would it do without records of payroll, invoices, inventory or accounts payable?

In rare cases, such loss of data results from computer system sabotage. More commonly, it is the result of fire.

Either way, gathering lost information is a Herculean task that many fail to complete. Forty percent of firms in this predicament reportedly go out of business.

Slow roasting

The MVP-101 desktop safe from Mediavault, Inc. of East Rutherford N.J. was designed specifically to protect floppy disks and tapes. It reportedly can protect its contents for an hour in temperatures up to 1,700 degrees Farenheit. In one independent test, though, floppy disks could still be used after they were slowly roasted at lower temperatures for more than 12 hours.

MVP-101, *desktop safe for floppies*

MVP-101 was designed to meet the environment requirements of floppy disks, which are more sensitive than tapes, according to Avi Tzur, Mediavault's president and the safe's designer. "Floppy disks can handle a maximum temperature of 125°F and a maximum relative humidity of 80%," Tzur says.

Many safes can insulate against the heat, but not all protect against water, Tzur claims. Humidity is an important factor in fires. "Most safes undergo water strain from the firefighter's hoses," Tzur explains.

The MVP-101 is also lightweight, the vendor claims. Because some fire safes are modified with extra insulation, shipping and handling for these types of vaults can add to the safes' weight and cost, Tzur states. The 15-in.-square MVP-101 uses materials developed for space technology and weighs less than 70 lbs.

To protect against theft, the safe is said to have a virtually pickproof lock from Salem, Va.-based Medeco Security Locks, Inc. The $695 MVP-101 safe stores up to 115 5¼-in. or 135 3½-in. floppy disks. — REBECCA HURST

Circle Reader Service Number 116

Correction

The cover for the May 6 issue of *Computerworld Focus* was illustrated by Jose Cruz.

PRODUCT CHECKLIST

The **Disk Technician software security system** has debuted from **Prime Solutions, Inc.**

According to the vendor, the Disk Technician software system automatically prevents, detects, repairs and recovers hard-disk media failures before data is lost on the IBM Personal Computer XT, AT and PCjr systems and compatibles.

The system consists of a single 5¼-in. diskette and works on both hard and floppy disk drives.

Prime Solutions claims that the product checks every byte on the disk, occupied or not, for the soft error rate, track alignment, magnetic retentivity and the ability to read and write. All unsafe soft errors are either repaired or blocked, and any programs and data files in use are moved to a safe area before the files lose data.

Disk Technician costs $99.95 and comes with a 30-day unconditional money-back guarantee.

Prime Solutions, 1940 Garnet Ave., San Diego, Calif. 92109.

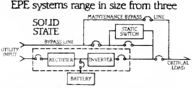
Circle Reader Service Number 117

Dial-Guard, Inc. has introduced the **Dial-Guard on-line security system.**

The Dial-Guard system is said to provide users with authentication and data protection. The system is made up of a hand-held Dial-Key, host-resident software and devices attached to terminals and personal computers. It uses dynamic one-time passwords and identifies users based on what they know, what they have and where they are.

Dial-Guard provides real-time message and electronic mail systems and creates custom management and audit reports. Optional message authentication coding and message encryptioo are available.

The basic system costs from $250 per protected terminal or PC, plus a software interface site license.



Dial-Guard, Suite 140, Building 1, 3000 Sand Hill Road, Menlo Park, Calif. 94025.

Circle Reader Service Number 118

Thoroughbred Software, a divisioo of Coocept Omega Corp., has rolled out **Thoroughbred Passport.**

Thoroughbred Passport enables value-added resellers to tie their proprietary software applications to a particular hardware system through the use of serial numbers, a method that does not restrict a user's ability to make backup copies, the company said.

Passport will be bundled with the company's Thoroughbred Basic under Unix and Microsoft Corp. Xenix and with Thoroughbred/OS, the company's proprietary operating system. The Passport device plugs into a serial port on the computer system.

Thoroughbred Passport is priced from $495 to $12,995, depending on computer system size.

Thoroughbred Software, P.O. Box 1035, 102 Old Camplain Road, Somerville, N.J. 08876.

Circle Reader Service Number 119

Black Box Corp. has rolled out the **Black Box Data Protector security device.**

The product has a proprietary cryptography coder that encrypts data before it is transmitted and decrypts the data when it is received at the other end, using the Data Encryption 5tandard algorithm.

The Black Box Data Protector supports most synchronous RS-232 personal computers and terminals, and it operates in either half- or full-duplex modes at selectable data rates of 110 bit/sec. to 9.6K bit/sec.

Black Box Data Protector costs $495

Black Box, P.O. Box 12800, Pittsburgh, Pa. 15241.

Circle Reader Service Number 120

Topaz, Inc. has announced the **Powermaker Micro UPS off-line system**

The Powermaker Micro UPS is an off-line uninterruptable power supply (UPS) system that reportedly provides the protection of an on-line UPS. It consists of a power conditioner, battery charger, battery, inverter, static transfer switch and a surge-suppression network

According to Topaz, the unit provides 100db of common-mode noise attenuation and 70db of normal-mode noise attenuation. It corrects voltage fluctuations as large as plus or minus 20% nominal voltage to within plus 6% to minus 8%.

If commercial power fails, the UPS inverter is said to switch on and begin supplying steady, noise-free AC power to the protected equipment in less than 1 msec Powermaker Micro UPS is available in power ratings of 1.8kVA and 1.5kVA in models with or without power conditioning

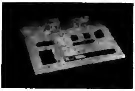
Prices for Powermaker start at $2,550.

Topaz, 9192 Topaz Way, San Diego, Calif. 92123.

Circle Reader Service Number 121

Cylink Corp. has announced the **Faxlok facsimile machine encryptor**

Faxlok is an encryption device designed to work with most Group III facsimile machines. The unit sends either encrypted or clear text with no reduction in message quality, according to Cylink. It also supports unattended facsimile operation.



Faxlok *fax machine encryptor*

Faxlok is priced at $2,450 per unit

Cylink, 920 W. Fremont Ave , Sunnyvale, Calif. 94087.

Circle Reader Service Number 122

Unisys Corp. has unveiled **Infoguard security software**.

Infoguard allows Unisys A series mainframe users to identify a security administrator who has exclusive authority to establish and maintain the security environment.

Infoguard is available through a five-year extended-term purchase priced from $8,450 or on a monthly license basis priced from $250.

Unisys, P.O. Box 418, Detroit, Mich 48232.

Circle Reader Service Number 123

Racal-Vadic, Inc. has released the **VA930 Callback Security System.**

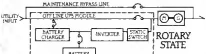
The VA930 Callback Security System is internal to Racal-Vadic's MDS-II System Controller chassis and protects host computers from unauthorized access.

The system provides three levels of access security: standard callback that calls back work-at-home employees at a phone number stored in the VA930 data base; programmed callback that enables traveling employees to specify a callback number during initial call-in; and pass-through access that connects authorized users directly to the host without callback.

The VA930 is priced at $2.995.

Racal-Vadic, 1525 McCarthy Blvd , Milpitas, Calif 95035.

Circle Reader Service Number 124



HOT SEAT

The following questions were solicited from users and conveyed to vendors for responses

Why did IBM go with a 31-bit addressing scheme instead of a 32-bit one for its MVS/XA system?

Felix M. Robbins
Robbins Consulting
Houston

Tom Belz, senior communications specialist, IBM: The answer to the question appears in the article titled "System/370 Extended Architecture: Design Considerations" by A. Padegs in the *IBM Journal of Research and Development* [Vol. 27 Number 3, May 1983]. I am quoting from page 201:

"The process to introduce 31-bit addressing into System/360-System/370 architecture started in the late 1960s when the new program status word and control register formats were established.

Although it was clear at the outset that an entire 4-byte field would have to be allocated for the extended address, the decision subsequently had to be made whether to use 31-bit addresses or continue with the 32-bit format introduced on the Model 67. The 31-bit format was chosen so as to provide space (high-order bit position) for a control or escape bit within the 4-byte address field. It was felt that the ability to address 4G bytes of storage with a 32-bit address instead of 2G bytes with a 31-bit address did not justify the potential inconvenience in the handling of the control or mode bits."

How do you convert from Prime Computer, Inc.'s Inform data base to an ASCII format?

Harry Bass
Bass Brothers, Inc.
Dallas

Joe Burke, group marketing manager, Prime: The question is a broad one, so I have made some assumptions about your intentions in asking it and have replied based on each set of assumptions.

Inform is the report generator within Prime's Prime Information data base management product and does not, by itself, have anything to translate, although its output may be saved and translated. Instead, you may be intending to translate a data file from within Prime Information itself.

Also, ASCII may be either a simple SAM or "flat" file (Prime Information files are segmented on the disk) or 8-bit ASCII format and not the 7-bit ASCII format that Prime utilizes on its computer systems.

Let's begin with the easiest interpretation of the question: producing a report and creating a SAM file. When you run Inform, you may generate the report to the spooler or to a hold file by adding LPTR (line printer) to the Inform statement and adjusting your assigned printer using the SETPTR command. The report that is generated already exists as an image-ready flat file, and you may edit, copy, print or download it in this condition.

To convert an existing Prime Information file of segmented variety to a flat file simply create a new data file, choosing a TYPE 1 from the type list that appears with the CREATE.FILE command. The TYPE 1 file accommodates records in a SAM format, and you may now simply execute a COPY command to move records from one file format to another.

To convert a Prime Information file to an 8-bit ASCII format requires a little programming. You would have to write a short Info/Basic program calling a Fortran, Cobol or PL/1 subroutine. The program would select the data records that you wanted to convert from a file and pass them to the subroutine, which would do an upper bit conversion and write the data to the output device, whether that device is a printer, tape drive or another system. A future release of Prime's Primos operating system will provide a facility to perform this operation more efficiently.

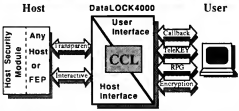
If the object of this exercise is to download data files to a personal computer, the job gets much easier using two existing Prime products. Prime has a product called Primelink, which does ASCII conversion automatically and transparently, allowing you to move files between a Prime system and a DOS-based processor.

There is also a version of the Prime Information data base environment available from Prime that runs on Microsoft Corp. MS-DOS 2.1 or higher. This version allows the personal computer user to access superminicomputer files transparently in real time and execute the ASCII conversion automatically.

The Hot Seat column consists of product- and service-related questions that you, our readers, would like us to ask a particular vendor.

Call us, toll free, at 1-800-343-6474 if you have a question. Or, forward your inquiries to Lory Zottola, Managing Editor, *Computerworld Focus*, 375 Cochituate Road, Box 880, Framingham, Mass. 01701-9171.

You'll never know unless you ask.



Blue Beat

Continued from page 51

and sophisticated communications. As the level of interaction between systems increases, so do the dangers of security breaches. So as technology advances, security systems must advance, too.

But MIS managers can't tackle the job alone. They must convince IBM and other vendors, who are moving full steam ahead on improving communications between various architectures, that they must also spend time improving security.

IBM is aware that technological innovation brings a greater chance of security breaches. While the company does offer a number of security options — including the RACF for mainframes — it is hesitant to educate its users to this fact.

IBM's reluctance

The reticence of IBM and other vendors lies in the fact that raising security concerns is not a positive selling approach. Nor are these companies eager to add to the cost of a large installation — strong security systems can be expensive, and installation and training can be lengthy processes.

Nevertheless, IBM sales representatives must commit to working with users to develop adequate security systems. In turn, users must insist that they receive proper help.

Many managers aren't even aware of the threat that new IBM technology poses.

While they're busily digesting the reams of technical information involving Systems Application Architecture (SAA), Token-Ring enhancements and the Personal System/2, few MIS managers are analyzing the security changes necessitated by this technology.

Under SAA, for instance, users will be able to access far more mainframe data from a personal computer than ever before. Without a proper security system, that could pose a serious problem.

Before installing any new technology, IBM or otherwise, MIS departments must do a complete risk analysis. This study can only be done effectively if it is performed in conjunction with a vendor that understands the security shortcomings of its system.

Managers must also take into account human shortcomings so they know when and where data security breaks are likely to occur and who is likely to commit them.

These two groups must work together to assure that strategies for dealing with potential risks are put into place as the technology itself is installed.

> **Many managers aren't even aware of the threat that new IBM technology poses.**

But technical solutions aren't always the answer.

Just as IBM assists in installation and system training, it must work with companies and users to launch serious educational programs that address security issues. An effective system means that users at all levels must be made aware that it exists.

The first group to educate must be the corporate staff. Strong support from corporate managers is essential for an effective security system.

Not only must upper level management foot the bill for a system, but it must also throw its weight solidly behind it so that security is taken seriously at all levels of the the company.

All of this is a big job — too big for the MIS departments to take on alone. IBM support for such projects is essential, both technologically and psychologically. The alternative is decidedly unattractive — businesses that can't protect their data from anyone — and television shows that promote this shortcoming.

Depke is editor of "IBM Watch," a biweekly newsletter published by IDG Communications, Inc.

CALENDAR

June 14-20

Localnet East Exhibition and Conference. New York, June 15-17 — Contact: Carol Peters, Online International, Inc., 989 Avenue of the Americas, New York, N.Y. 10018.

Network Protocols and Standards. San Francisco, June 15-17 — Contact: Systems Technology Forum, Suite 150, 10201 Lee Highway, Fairfax, Va. 22030.

Local Communications Systems. Dallas, June 15-17 — Contact: Systems Technology Forum, Suite 150, 10201 Lee Highway, Fairfax, Va. 22030.

The National Computer Conference (NCC). Chicago, June 15-18 — Contact: NCC '87, American Federation of Information Processing Societies, Inc., 1899 Preston White Drive, Reston, Va. 22091.

The Third International Integrated Services Digital Networks Exposition. Atlanta, June 15-19 — Contact: Christopher Kennelly, Information Gatekeepers, Inc., 214 Harvard Ave., Boston, Mass. 02134.

Telecommunications Management. Dallas, June 17-19 — Contact: Business Communications Review, 950 York Road, Hinsdale, Ill. 60521.

Data Networks: Management, Operation and Control. Arlington, Va., June 17-19 — Contact: Technology Transfer Institute, 741 Tenth St., Santa Monica, Calif. 90402.

Releasing the Power of PC-DOS/MS-DOS. Morristown, N.J., June 18-19 — Contact: The American Institute, Carnegie Building, 55 Main St., Madison, N.J. 07940.

Telecommunications Management Software: How to Plan and Select. New York, June 18-19 — Contact: Business Communications Review, 950 York Road, Hinsdale, Ill. 60521.

IBM Product Strategies and Architectures. Philadelphia, June 18-19 — Contact: Data-Tech Institute, P.O. Box 2429, Lakeview Plaza, Clifton, N.J. 07015. Also being held June 25-26 in Boston.

June 21-27

Essential Systema Development: A Fourth-Generation Methodology. San Francisco, June 22-24 — Contact: Technology Transfer Institute, 741 Tenth St., Santa Monica, Calif. 90402.

Network Design. New York, June 22-24 — Contact: Systems Technology Forum, Suite 150, 10201 Lee Highway, Fairfax, Va. 22030.

Managerial Planning for the Security and Privacy of Contemporary Computer and Telecommunications Systems. Cambridge, Mass., June 22-26 — Contact: Office of the Summer Session, Room E19-356, 50 Ames, Massachusetts Institute of Technology, Cambridge, Mass. 02139.

Contract Negotiation and System Implementation. Atlanta, June 25-26 — Contact: Business Communications Review, 950 York Road, Hinsdale, Ill. 60521.

Understanding and Selecting Voice Messaging Systems. Seattle, June 25-26 — Contact: Business Communications Review, 950 York Road, Hinsdale, Ill. 60521.

June 28-July 4

T1 Networking. Dallas, June 29-July 1 — Contact: Systems Technology Forum, Suite 150, 10201 Lee Highway, Fairfax, Va. 22030.

Voice/Data PBXs. Washington D.C., June 29-July 1 — Contact: Systems Technology Forum, Ste. 150, 10201 Lee Highway, Fairfax, Va. 22030.

SALES OFFICES

Publisher/President/Lee Vidmer

Vice President/Sales/Edward P. Marecki **COMPUTERWORLD** 375 Cochituate Road Box 9171 Framingham MA 01701-9171 (617) 879-0700

BOSTON SALES OFFICE Northern Regional Manager/Michael F. Kelleher **District Managers**/David Peterson Bill Cadigan Sherry Driscoll **Account Manager**/John Watts **Sales Assistant**/Alice Longley **COMPUTERWORLD** 375 Cochituate Road Box 9171, Framingham M4 01701-9171 (617) 879-0700

CHICAGO SALES OFFICE Midwest Regional Manager/Russ Gerches **District Managers**/Kevin McPherson Larry Craven **Sales Assistant**/Kathy Sullivant **COMPUTERWORLD** 2600 South River Road Suite 304 Des Plaines IL 60018 (312) 827-4433

NEW YORK SALES OFFICE Eastern Regional Director/Michael J. Masters **Senior District Manager**/Doug Cheney **District Managers**/Fred Lo Sapio Frank Genovese **Account Manager**/Paula Smith **Sales Assistants**/Mary Tagliareni Sue Larson **COMPUTERWORLD** Paramus Plaza I 140 Route 17 North Paramus NJ 07652 (201) 967-1350

LOS ANGELES SALES OFFICE Western Regional Director/William J. Healey **District Manager**/Carolyn Knox **COMPUTERWORLD** 18004 Sky Park Circle Suite 255 Irvine C4 92714 (714) 261-1230

SAN FRANCISCO SALES OFFICE Western Regional Director/William J. Healey **Senior District Manager** Barry Milione **District Managers**/Ernie Chamberlain Mark V. Glasner Stevan Phillips **Account Manager** Alicia Hodge **COMPUTERWORLD** 300 Broadway Suite 20 San Francisco CA 94133 (415) 421-7330

ATLANTA SALES OFFICE Eastern Regional Director/Michael J. Masters **District Manager**/Jeffrey Melnick **Sales Assistant**/Melissa Christie **COMPUTERWORLD** 1400 Lake Hearn Drive Suite 330 Atlanta GA 30319 (404) 394-0758

DALLAS SALES OFFICE Midwest Regional Manager/Russ Gerches **District Manager**/Kevin C. Harold **COMPUTERWORLD** 14651 Dallas Parkway Suite 304 Dallas TX 75240 (214) 233-0882

WASHINGTON D C SALES OFFICE Eastern Regional Director/Michael J. Masters **District Manager** Bernie Hockswender **COMPUTERWORLD**, 3022 Javier Road #210 Fairfax V4 22031 (703) 280-2027

PRODUCT CLASSIFIED ADVERTISING Product Classified Advertising/Account Manager Peter Slinguff 375 Cochituate Road Box 9171 Framingham M4 01701-9171 (617) 879-0700

RECRUITMENT ADVERTISING National Recruitment Sales Director/John Corrigan 375 Cochituate Road Box 9171 Framingham M4 01701-9171 (617) 879-0700

RECRUITMENT ADVERTISING SALES OFFICES
New England Recruitment Manager/Al DeMille
375 Cochituate Road Box 9171 Framingham, MA 01701-9171 (617) 879-0700

New York Recruitment Manager/Warren Kolber
Paramus Plaza 1 140 Route 17 North Paramus NJ 07652 (201) 967-1350

Midwest
2600 S. River Road Suite 304 Des Plaines IL 60018 (312) 827-4433

Western Recruitment Manager/Barbara Murphy
18004 Skypark Circle Suite 100 Irvine CA 92714 (714) 250-0164

Mid-Atlantic Recruitment Manager/Kathryn Kress
3110 Fairview Park Drive Suite 1040 Falls Church V4 22042 (703) 876-5100

RECRUITMENT TELEMARKETING ACCOUNT EXECUTIVES
New England, New York/Jay Novack **Mid-Atlantic**/Pauline Smith
Midwest/Ellen Casey **Western**/Nancy Percival
Toll Free 1-800-343-6474 or (617) 879-0700

Advertisers Index

Page number	Advertiser
48	Amdahl Corp *800 538 8460*
C4	Applix Inc *617-870 0300*
8 9 38-39	AT&T *1 800 CLP INFC*
50	Business Software Inc *404 449 3200*
11	Chicor *312 454 9670 203 359 5639*
C2	Comdisco *312 698 3000*
56	Compusource *919 469 3325*
12	Computer Associates *800 645 3003*
57	CW Circulation *617-879-0700*
36	CW Focus *617-879 0700*
24	DataGuard *800 433 0339 in OHIO 1 216 526 6373*
4	Data General Corp *1 800-DATAGEN 1 800 268 5454*
34	Datasphere *1 800-221 0575 in NJ call 201 382 2300*
2-3,46	Digital Equipment Corp
30	*E4C*
18	Electrorep Datacomm *516 752 0585*
54-55	Emergency Power Engineering *714 557 1636*
44	Emerson *1 800-BACKUPS ext 28 714 545 5581*
50	Equicor Technologies *215 861 2800*
16	Fisher International *800 237 4510 in Florida 813 643 1500*
31,58	Goal Systems *1 800-848 4640*
29	Gould *1 800 GOULD 10*
19	Harris Corp *800-4 HARRIS ext 4021*
42-42	IDG Corporate *617 875-5000*
22	Imulec *516 581 6803*
14	Liebert Corp *614-888 0246*
40	Local Data *213 320 7126*
47	LPC *800 852-0852 312 932 7000*
56	MicroFrame *609 395 7800*
40	Micro Security *801 972-0579*
26,28	Mosaic Computer Security *617 491 2434*
32	On-Line Systems *800 642 0177*
34	Provident *919 481 0011*
11	Software Technology & Research/STAR *1 800 258 STAR in CT 203 529 7728*
10	Stratus *617 460 2192*
6	Sunguard *800 523 4970*
6	Techland *800 TECHLAN in NY 212 684 7788*
7	VM Software, Inc *800 562 7100 703 264 8000*
52-53	Xerox Corp *800 TEAM XRX ext 1876*

This index is provided as an additional service. The publisher does not assume any liability for errors or omissions.

log off

Snow and
Ice storm .005 - 10.0 Same as for hurricane plus roof heating
snow removal plans.
Tornado 2.05*10-9 - 2.6*10 Same as for hurricane plus personnel
and pressure release vents.
Air-
Conditioning
Failure .2 - 5.0 Backup for air-conditioning chillers and
equipment. Alarms on the air
maintenance and monitoring.
Data entry
Errors not available Data validation routines.
Electrical
Fire .001 - .004 hot site; cold site.
Maintenance procedures; backup; redundancy;
physical security of the hardware.
Operator
Failure 10. - 200. Hiring and training procedures; operational procedures; error checking software; security packages.

BRUCE SANDERS

Backing up PC data

Thomas Roberts

During the past five years, an estimated 12 million personal computers have been installed in U.S. businesses. This PC boom has revolutionized the way people work with corporate data. Information that once took days to get is now often available immediately and can be manipulated by most any PC user.

The positive effect of this democratization of corporate data is that decisions are made more efficiently. However, there has also been a negative effect on the way corporate information is treated. Stand-alone PCs have made it much harder to maintain data's security and integrity.

Take, for instance, the simple problem of hard-disk backup. With traditional shared-storage systems, MIS would manage, back up and be accountable for the data stored on a system. With stand-alone PCs, however, the process must be entrusted to each user instead, and the majority of PC users remain astoundingly disinterested in backing up their data.

Sensitive data can also fall prey to more malicious intentions. An employee leaving the company may decide that information stored on a PC would be helpful in a new job. PC floppy disks offer an excellent means by which to take a great deal of information out of an office.

The search for a solution to these problems has led many an MIS director to the conclusion that hooking PCs into a centralized hub, such as a local-area network (LAN) server or departmental computer, will help harness the flow of PC-based information by providing a centralized spot for data to be stored.

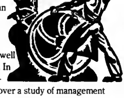
How much control a LAN server or departmental system can lend to an environment of stand-alone PCs depends on the sophistication of its operating system software. However, some LAN operating systems (Novell, Inc.'s Advanced Netware, for example) are beginning to offer facilities for automatic backup of data stored on connected PCs.

But connecting standard PCs to a LAN or departmental system will do nothing about a user's ability to transfer sensitive data to floppies. Diskless PCs propose a way to solve this problem. As with dumb terminals, diskless workstations force all data storage and management to be handled centrally. Although users with diskless PCs cannot store files locally, they retain some of the performance benefits of distributed processing.

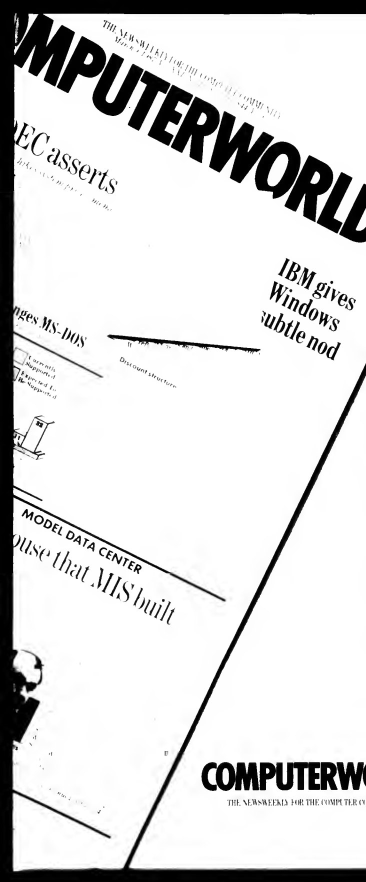
However, it is important for users to realize that they owe much of the PC's performance advantage to fast local storage. When relying on centralized storage, a diskless PC user will be directly affected by both the speed of the link to the central system and the number of users on that system. Local hard-disk storage is all but becoming a necessity for more sophisticated PC applications that are growing in size and complexity.

Roberts is manager of personal computer research at International Data Corp., a Framingham, Mass.-based industry research firm

next issue



Software in the summer. July's *Focus* examines an array of software productivity tools and trends. We'll look at AI and high-end application generators as well as user interface management systems. In addition to software development, engineering and maintainence, *Focus* will cover a study of management in the 1990s. Meet the new kids on the equipment and services block, and check out IBM's Personal System/2 strategy. Don't let the lazy days of summer keep you from making the most of your software!



EVERYBODY ON THIS LIST GETS COMPUTERWORLD TOO LATE.

If you're on the office route slip, you're getting COMPUTERWORLD too late.

You need to know the most up-to-date news in the computer field as it happens. Hot off the presses. While you can still use it.

COMPUTERWORLD keeps you on top of all the latest news, products, people, developments, trends, ideas and issues. Plus, we've expanded our coverage of microcomputing and networking, and we've added SPOTLIGHT — a handy pull-out section that can be saved for future reference.

Each SPOTLIGHT features a particular product category with surveys of key vendors and tables outlining prices, vendors and specifications. Plus, with DAIL INQ you can request information about products in SPOTLIGHT with just one phone call!

So get off the route slip and get your own copy of COMPUTERWORLD for just 76¢ a week! That's $38.95 for 51 weekly issues of COMPUTERWORLD, plus 12 issues of Computerworld Focus — FREE. Each FOCUS issue provides in-depth coverage of a current hot topic such as information centers, PCs, software, and more.

Subscribe today! Call toll free **1-800-544-3712** (in PA, call collect 215 768 0388) or use the convenient postage-paid order cards in this issue.

COMPUTERWORLD

THE NEWSWEEKLY FOR THE COMPUTER COMMUNITY

At Last. An Office Software System for the Highest Common Denominator.

Alis. Designed for the professional office.

If your company's success hinges on the work of professionals, the engineer, the business professional, the scientist, we have a suggestion to make

Consider Alis The office software system designed specifically for the professional office

It networks workstations, PCs and terminals company-wide So your professionals have the time to do the job they were hired to do, and their staff gets professional-looking results quickly and easily

Spend more time on the job. And less on paperwork.

Studies show that many business and engineering professionals spend more than 50% of their time on administrative tasks Chances are, it's not much different in your firm

Reducing that percentage of non-productive time is what Alis is all about Because Alis combines the benefits of communications-based office automation systems with the advantages of graphics-based personal computer applications

Alis is available right now.

On equipment your people use right now Apollo, Compaq, Digital VAX, Hewlett-Packard, Honeywell, IBM RT PC, Masscomp, NCR Tower, and Sun Chances are Alis can be networked across them with complete transparency For example, VAXs and 68000-based workstations and MS-DOS PCs

To find out more, contact your local representative of the companies mentioned above
Or call Mike Beringer, V P North American Sales,
at Applix (617) 870-0300

Alis combines text spreadsheets graphics and database in single always editable documents □ handles proportionally spaced and multiple-size fonts WYSIWYG style □ provides automatic formatting of reports letters memos etc □ sophisticated equation solving spreadsheet □ drawing scanned images and business graphics □ personal and office databases □ integrated electronic mail and meeting scheduling □ multiple windows □ supports graphic workstations PCs and terminals

Alis AppliXA and Applix are registered trademarks of Applix Inc
RT PC is a trademark of International Business Machines Inc
VAX is a registered trademark of Digital Equipment Corporation
MS-DOS is a trademark of Microsoft Corporation

from *APPLIX*®

The integrated software system for the professional office.

Finally, some answers in Wonderland.

APPLIX INC 112 TURNPIKE ROAD, WESTBORO, MASSACHUSETTS 01581 (617) 870-0300

Circle Reader Service Number 83